

Kaseya 2

Virtual System Administrator™

Benutzerhandbuch

Version 7.0

Deutsch

January 28, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

Datenbanksichten 477

API-Web-Services 531

Kapitel 1

Konfiguration

In diesem Kapitel

Konfiguration des Servers

Der Server ist das Herz des Systems. Die Benutzer greifen auf alle Funktionen über die Weboberfläche dieses Servers zu. Die Agents auf allen verwalteten Rechnern stellen eine Verbindung zu diesem Server her, um Anleitungen bzw. Anweisungen für Aufgaben zu erhalten. Ihr Server muss Benutzern und Agents gleichermaßen zur Verfügung stehen.

Informationen zur Konfiguration des Servers finden Sie in den aktuellsten **Installationsanweisungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/install/index.asp#home.htm)*.

Systemsicherheit

Das System wurde in jeder Hinsicht für optimale Sicherheit entwickelt. Unser Designteam hat mehr als 50 Jahre an Erfahrung im Entwerfen sicherer Systeme für Regierungs- und Geschäftsanwendungen. Dank dieser Fachkenntnisse konnten wir Benutzerfreundlichkeit und höchste Sicherheit auf einzigartige Weise kombinieren.

Die Architektur der Plattform stellt einen wesentlichen Bestandteil der Sicherheit dar. Dieser Agent leitet alle Kommunikationen zurück zum Server. Da er *keine eingehenden Verbindungen akzeptiert*, sind keinerlei Angriffe auf den Agent durch eine Drittanbieteranwendung über das Netzwerk möglich. *Das System benötigt keine geöffneten Eingabeports* an den verwalteten Rechnern. Daher kann der Agent seine Aufgabe in praktisch jeder Netzwerkkonfiguration durchführen, ohne Anfälligkeit an eingehenden Portsensoren oder neue Netzwerkangriffe zu verursachen.

Der VSA schützt vor Man-In-The-Middle-Angriffen, indem die gsamte Kommunikation zwischen Agent und Server mit AES-256-Bit-RC4-Verschlüsselung gesendet wird. Der Schlüssel wird jedes Mal geändert, wenn der Server eine Aufgabe an den Agent überträgt, also mindestens einmal am Tag. Da keine Datenpakete im Klartextformat im Netzwerk übertragen werden, sind keine sogenannten „Exploits" für einen Angreifer vorhanden.

Benutzer greifen nach einem sicheren Anmeldeprozess über eine Weboberfläche auf den VSA zu. Das System sendet niemals Passwörter über das Netzwerk und speichert sie nie in der Datenbank. Nur der Benutzer kennt sein jeweils eigenes Passwort. Der Client kombiniert das Passwort mit einer zufälligen Kontrollfrage, die vom VSA-Server für jede Sitzung ausgegeben wird, und hashcodiert dies mit SHA-256. Der Server testet dieses Ergebnis, um den Zugriff zu gewähren oder zu verweigern. Diese einzigartige zufällige Kontrollfrage schützt vor Man-In-The-Middle-Angriffen, bei denen das Netzwerk ausgeschnüffelt wird und die willkürlichen Elemente erfasst werden, die dann später zum Zugriff auf den VSA verwendet werden.

Als letzte Maßnahme für maximale Sicherheit unterstützen VSA-Webseiten den Betrieb als SSL-Website.

Mindestsystemanforderungen

Informationen dazu finden Sie in den aktuellen **Mindestsystemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Upgrades oder Aktualisierungen des VSA

Aktuelle Informationen zum Upgrade aus einer früheren Version von Kaseya auf die aktuelle Version oder dem Upgrade eines vorhandenen K2-Servers auf die aktuelle Version finden Sie in den **Installationsanweisungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/Install/index.asp#home.htm)*.

Anmeldungs- und Browsereinstellungen

So melden Sie sich bei Virtual System Administrator™ an

1. Gehen Sie in Ihrem Browser zur Anmeldeseite des VSA-Servers.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.

> **Hinweis:** Zur erstmaligen Anmeldung verwenden Sie den Kontonamen und das Passwort des Hauptbenutzers, die bei der Installation festgelegt wurden.

3. Aktivieren Sie das Kontrollkästchen **Meinen Benutzernamen und meine Domäne (falls vorhanden) auf diesem Computer speichern**, damit der Benutzer- und der Domainname in einem Cookie auf dem lokalen Rechner gespeichert werden und Sie sie nicht bei jeder Anmeldung erneut eingeben müssen.

> **Hinweis:** Das Zusatzmodul für **Discovery** kann zur Verwaltung von VSA-Anmeldedaten für Benutzer und für den Portalzugriff mithilfe von **Domänenanmeldedaten** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#7293.htm)* verwendet werden.

4. Klicken Sie auf die Schaltfläche **Login**.

> **Hinweis:** Um nach einer Änderung der Konfiguration einen nicht autorisierten Zugriff zu verhindern, melden Sie sich ab oder schließen die Sitzung, indem Sie die Browseranwendung beenden.

Browser-Cookies, JavaScript und Popups aktivieren

In Ihrem Browser müssen Cookies und JavaScript aktiviert sein. Außerdem wird empfohlen, Popups für die VSA-Website zuzulassen.

Internet Explorer

So aktivieren Sie Cookies in Internet Explorer 9, 10 und 11

1. Klicken Sie auf das Menü **Extras** bzw. das Zahnradsymbol.
2. Wählen Sie **Internetoptionen** aus.
3. Öffnen Sie die Registerkarte **Datenschutz**.
4. Wählen Sie eine Datenschutzeinstellung nicht höher als **Mittelhoch** (also weder die Einstellung 'Hoch' noch 'Alle Cookies sperren').
5. Klicken Sie auf **OK**.

So aktivieren Sie JavaScript in Internet Explorer Internet Explorer 9, 10 und 11

1. Klicken Sie auf das Menü **Extras**.
2. Wählen Sie **Internetoptionen** aus.
3. Wechseln Sie zur Registerkarte **Sicherheit**.
4. Klicken Sie unter **Wählen Sie eine Zone von Webinhalten, um die Sicherheitseinstellungen dieser Zone festzulegen** auf **Internet**.
5. Klicken Sie auf **Stufe anpassen...**.
6. Scrollen Sie herunter zum Abschnitt **Scripting**.
7. Klicken Sie unter **Skripting von Java-Applets** auf **Aktivieren**.
8. Klicken Sie auf **OK**.

So aktivieren Sie Popups in Internet Explorer 9, 10 und 11:

1. Klicken Sie auf das Menü **Extras**.
2. Wählen Sie **Internetoptionen** aus.
3. Öffnen Sie die Registerkarte **Datenschutz**.
4. Wählen Sie **Einstellungen**. Das Dialogfeld **Popupblockereinstellungen** wird angezeigt.
5. Geben Sie die URL oder IP-Adresse Ihres VSA in das Feld **Adresse der Website, die zugelassen werden soll** ein.
6. Klicken Sie auf **Schließen** und anschließend auf **OK**.

Firefox

So aktivieren Sie Cookies in Firefox:

1. Klicken Sie auf das **Firefox**-Menü.
2. Wählen Sie **Einstellungen**.
3. Gehen Sie zu den Einstellungen für **Datenschutz**.
4. Setzen Sie die Chronik auf **Firefox wird eine Chronik: anlegen**. (Sie können auch **Firefox wird eine Chronik: nach benutzerdefinierten Einstellungen anlegen** wählen und die Option **Cookies akzeptieren** aktivieren.)
5. Klicken Sie auf **OK**.

So aktivieren Sie JavaScript in Firefox:

1. Klicken Sie auf das **Firefox**-Menü.
2. Wählen Sie **Einstellungen**.
3. Öffnen Sie die Registerkarte **Inhalt**.
4. Aktivieren Sie das Kontrollkästchen **JavaScript aktivieren**.
5. Klicken Sie auf **OK**.

So aktivieren Sie Popups in Firefox:

1. Klicken Sie auf das **Firefox**-Menü.
2. Wählen Sie **Einstellungen**.
3. Öffnen Sie die Registerkarte **Inhalt**.
4. Wählen Sie **Ausnahmen...** Das Dialogfeld **Berechtigte Websites – Pop-ups** wird angezeigt.
5. Geben Sie die URL oder IP-Adresse Ihres VSA in das Feld **Adresse der Website** ein.
6. Klicken Sie auf **Erlauben**.
7. Klicken Sie auf **Schließen** und anschließend auf **OK**.

Chrome

So aktivieren Sie Cookies in Chrome:

1. Klicken Sie auf das **Chrome**-Symbol.
2. Wählen Sie **Einstellungen**.
3. Klicken Sie auf **Erweiterte Einstellungen anzeigen**.
4. Klicken Sie im Abschnitt **Datenschutz** auf **Inhaltseinstellungen**.
5. Wählen Sie die Option **Speicherung lokaler Daten zulassen (empfohlen)**.
6. Klicken Sie auf **Fertig** und schließen Sie alle übergeordneten Dialogfelder.

So aktivieren Sie JavaScript in Chrome:

1. Klicken Sie auf das **Chrome**-Symbol.

2. Wählen Sie **Einstellungen**.
3. Klicken Sie auf **Erweiterte Einstellungen anzeigen**.
4. Klicken Sie im Abschnitt **Datenschutz** auf **Inhaltseinstellungen**.
5. Gehen Sie zum Abschnitt **JavaScript**.
6. Aktivieren Sie die Option **Ausführung von JavaScript für alle Websites zulassen (empfohlen)**.
7. Klicken Sie auf **Fertig** und schließen Sie alle übergeordneten Dialogfelder.

So aktivieren Sie Popups in Chrome:

1. Klicken Sie auf das **Chrome**-Symbol.
2. Wählen Sie **Einstellungen**.
3. Klicken Sie auf **Erweiterte Einstellungen anzeigen**.
4. Klicken Sie im Abschnitt **Datenschutz** auf **Inhaltseinstellungen**.
5. Gehen Sie zum Abschnitt **Pop-ups**. (Möglicherweise müssen Sie im Dialogfeld nach unten scrollen.)
6. Aktivieren Sie die Option **Anzeige von Pop-ups für keine Website zulassen (empfohlen)**.
7. Klicken Sie auf **Ausnahmen verwalten...** Das Dialogfeld **Ausnahmen für Pop-ups** wird angezeigt.
8. Geben Sie die URL oder IP-Adresse Ihres VSA in das Feld **Muster für Hostname** am Ende der Liste ein.
9. Setzen Sie das **Verhalten** auf `Erlauben`.
10. Klicken Sie auf **Fertig** und schließen Sie alle übergeordneten Dialogfelder.

Kapitel 2

Erste Schritte

In diesem Kapitel

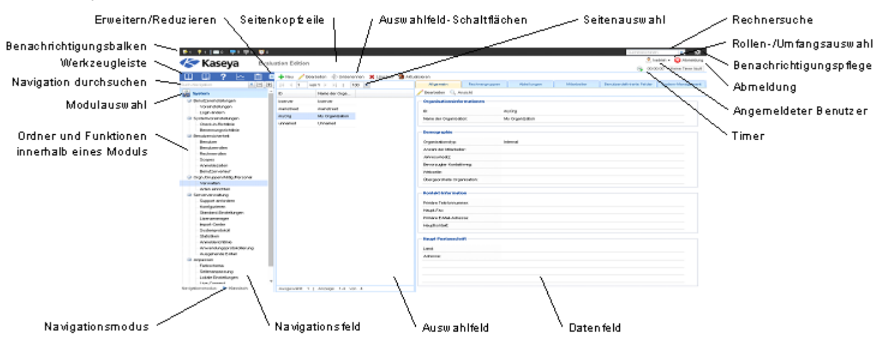
VSA-Module

Alle VSA-Funktionen können über Module aufgerufen werden, die auf der linken Seite der Benutzeroberfläche aufgelistet sind. Innerhalb jedes Moduls befinden sich die Kernfunktionen, mit denen Benutzer eine Reihe von Aufgaben auf remote verwalteten **Rechnern** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#6779.htm)* und dem Kaseya Server ausführen können.



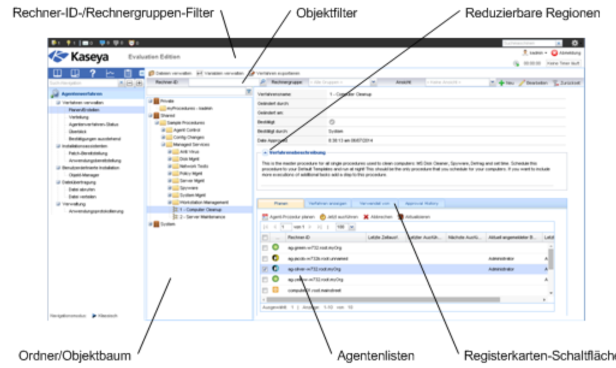
Page Layout

Die Benutzeroberfläche von Kaseya 2 ist sehr flexibel. Gleichzeitig macht sie es für den Benutzer einfach, die erforderlichen Auswahlen zu treffen.



- **Navigationsfeld** – Die Registerkarten und Funktionsfelder des Moduls werden zu einem einfachen Navigationsfeld im Stil des Windows Explorers zusammengefasst, das nach Bedarf erweitert oder reduziert werden kann.
- **Navigationsmodi** – Zwei Modi stehen zur Verfügung:
  - **Baumstruktur** – Sie können die einzelnen Ordner innerhalb eines Moduls auswählen und erweitern.
  - **Klassisch** – Zeigt zu jedem Zeitpunkt nur jeweils ein Modul an. Alle Ordner sind standardmäßig erweitert. Alle Ordner sind standardmäßig reduziert und können einzeln erweitert werden.
- **Auswahlfeld** – Für zahlreiche Funktionen in Kaseya 2 wird ein mittleres Auswahlfeld angezeigt, in dem Sie einen oder mehrere Datensätze auswählen können. Das Auswahlfeld kann gescrollt, gefiltert und unabhängig von anderen Feldern sortiert werden.
- **Datenfeld** – Auf der rechten Seite des Bildschirms befindet sich ein Datenfeld, das als eine Reihe von Registerkartenansichten ausgelegt ist, die schnellen Zugriff auf die Eigenschaften sämtlicher Datenansichten bieten, egal wie komplex eine Funktion sein mag. Auf zahlreichen der Registerkarten befinden sich bearbeitbare Felder und Schaltflächen, über die Sie weitere Funktionen aufrufen können.
- **Modulauswahl** – Im oberen Bereich des Navigationsfelds befindet sich eine Modulauswahl. Durch Klicken auf das sichtbare Modul werden alle installierten Module im VSA angezeigt. Wenn Sie auf eines der anderen Module klicken, wird dieses Modul ausgewählt. Außerdem werden alle Ordner und Funktionen innerhalb dieses Moduls angezeigt, für die der Benutzer Anzeigerechte besitzt.
- **Benachrichtigungsbalken** – Zeigt Status und Anzahl der Benachrichtigungskategorien an. Benachrichtigt Sie bei Aktualisierung eines angegebenen RSS-Feed.
- **Benachrichtigungspflege** – Passt die Anzeige von Benachrichtigungen nach Kategorie an.
- **Werkzeugleiste** – Die unmittelbar über der Modulauswahl befindliche Werkzeugleiste bietet umgehenden Zugriff auf die globalen Funktionen **Lesezeichen anzeigen**, **Lesezeichen hinzufügen**, **Hilfe**, **Status** und **Anmerkungen**. Diese Funktion kann über das Zahnradsymbol ⚙ rechts oben im **Benachrichtigungsbalken** *(siehe 11)* ausgeblendet werden.
- **Navigation durchsuchen** – Geben Sie einen Suchausdruck ein, um übereinstimmende Navigationselemente zu finden. Diese Funktion kann über das Zahnradsymbol ⚙ rechts oben im **Benachrichtigungsbalken** *(siehe 11)* ausgeblendet werden.
- **Erweitern/Reduzieren** – Mit dem Symbol **<<** rechts neben der Symbolleiste wird das Navigationsfeld reduziert. Über **>>** wird ein reduziertes Navigationsfeld wieder erweitert.
- **Auswahlfeld-Schaltflächen** – Im oberen Bereich des Auswahlfelds befindet sich eine seitenspezifische Schaltflächenleiste. Darin befinden sich in der Regel Schaltflächen zum Erstellen, Bearbeiten und Löschen der im Auswahlfeld aufgelisteten Datensätze. Abhängig von der Seite und Ihren Zugriffsrechten werden möglicherweise weitere Schaltflächen angezeigt.

- **Seitenauswahl** – Falls das Auswahlfeld über eine Seite hinausgeht, können Sie mithilfe der Seitenauswahl durch mehrere Seiten blättern. Sie können auch die Anzahl der Zeilen festlegen, die auf jeder Seite angezeigt werden.
- **Seitenkopfzeile** – In der oberen linken Ecke werden ein anpassungsfähiges Site-Logo und der Kopfzeilentext angezeigt.
- **Rollen-/Umfangsauswahl** – Damit wird die Kombination von Rolle und Umfang ausgewählt, die derzeit für Ihre Anmeldeinformationen aktiv ist. Falls Sie mehrere Rollen oder Umfänge verfügbar haben, können Sie jederzeit während Ihrer Anmeldesitzung die Rolle oder den Umfang wechseln.
- **Angemeldeter Benutzer/Abmelden** – Zeigt den Benutzernamen des gegenwärtig angemeldeten Benutzers sowie einen Abmeldelink an.
- **Ungelesene Nachrichten** – In der oberen rechten Ecke wird die Anzahl der ungelesenen Nachrichten angezeigt. Sie können jederzeit auf diesen Zähler klicken, um Ihren VSA-Posteingang anzuzeigen.
- **Timer** – Zeichnet Zeiteinträge auf, die in Arbeitszeittabellen und anderen Arbeitszeitnachweisen übernommen werden können.



- **Rechner-ID-/Rechnergruppen-Filter** – Falls auf einer Seite eine Agent-Liste angezeigt wird, erscheint am oberen Rand der Seite der Rechner-ID-/Rechnergruppen-Filter. Über diesen Filter können Sie die Liste der Agents, die auf dem Rechner angezeigt werden, nach Rechner, Rechnergruppe, Organisation oder Ansichtsdefinition beschränken.
- **Ordner-/Objektbäume** – Für bestimmte Funktionen wird im Auswahlfeld eine Ordnerbaumstruktur anstelle einer Liste von Datensätzen angezeigt. Normalerweise werden zwei Ordnerbäume bereitgestellt, ein **privater** und ein **gemeinsam genutzter**, doch mitunter wird auch nur der gemeinsam genutzte Ordnerbaum angezeigt. Sie können neue Objekte in diesen Ordnerbäumen erstellen. Im **gemeinsam genutzten** Ordnerbaum können Sie diese außerdem für andere Benutzer freigeben.
- **Baumfilter** – Alle Ordnerbaumfelder können durch Eingabe einer Zeichenfolge in den Baumfilter gefiltert werden.
- **Agent-Listen** – Auf zahlreichen VSA-Seiten werden Agent-Listen angezeigt. In der neuen Benutzeroberfläche werden Agents häufig auf einer der Registerkarten im Datenfeld im rechten Teil der Seite angezeigt.
- **Registerkartenspezifische Schaltflächen** – Auf jeder Registerkarte im Datenfeld im rechten Teil der Seite kann eine für diese Registerkarte spezifische Gruppe von Schaltflächen angezeigt werden. Registerkartenspezifische Schaltflächen bestimmen den darunter liegenden untergeordneten Datensatz. Angenommen, Sie wollen ein Agent-Verfahren sofort ausführen. In diesem Fall wählen Sie das Verfahren im Ordnerbaum im mittleren Feld aus. Anschließend wählen Sie einen oder mehrere Agent(s) auf der Registerkarte aus und klicken auf die registerkartenspezifische Schaltfläche "Jetzt ausführen", um das Agent-Verfahren auszuführen.
- **Reduzierbare Regionen** – Felder, Registerkarten und Dialogfelder werden mitunter in reduzierbare Regionen unterteilt. Durch Klicken auf den Pfeil nach unten wird diese Region auf der Benutzeroberfläche ausgeblendet. Für eine reduzierte Region wird eine Erweiterungsschaltfläche angezeigt, mit der Sie diese Region wieder erweitern können.

Benachrichtigungsbalken

Am oberen Rand des VSA-Fensters wird ein Benachrichtigungsbalken angezeigt, der in allen Modulen sichtbar ist. Über die Balkensymbole erhalten Sie sofortige Benachrichtigungen in der gesamten VSA-Umgebung.



Dazu gehören:

- **Service-Desk-Tickets** – Für verschiedene Desks, Desk-Gruppen oder andere Filterkriterien können mehrere Benachrichtigungssymbole erstellt werden.
- **RSS-Ankündigungen** – Für verschiedene RSS-Feeds können mehrere Symbole festgelegt werden.
- **Systembenachrichtigungen** – Umfasst Nachrichten der Systemebene mit den Stufen "kritisch" und "Warnung".
- **Posteingangsnachrichten** – Für verschiedene Arten von Posteingangsnachrichten können mehrere Symbole erstellt werden.
- **Agent-Zähler** – Wenn Sie auf einen dieser beiden Zähler klicken, wird ein Dialogfeld geöffnet, in dem Sie ein Agent-Installationspaket auswählen und sofort auf dem Computer installieren können, auf dem Sie gegenwärtig angemeldet sind.

Rechnersuche

Rechts neben dem Benachrichtigungsbalken befindet sich das Bearbeitungsfeld **Rechnersuche**. Geben Sie eine Zeichenfolge ohne Lehrstellen in das Feld ein. Alle Rechnernamen, die diese Zeichenfolge enthalten, werden in einer Dropdown-Liste angezeigt. Die Suchausdrücke werden mit den folgenden Arten von Daten abgeglichen.

- `display name`
- `current login`
- `last login name`
- `mach name`
- `admin contact`
- `contact name`
- `contact phone`
- `contact email`
- `ip address`
- `ipv6 address`
- `default gateway`
- `connection gateway ip`
- `primary wins server`
- `dns server 1`
- `dns serve 2`
- `os type`
- `os info`
- `mac addr`
- `org name`

- `group name`

Die Dropdown-Liste zeigt für jede ermittelte Rechner-ID die folgenden Informationen an:

- Rechnername
- Name des für diese Rechner-ID verantwortlichen VSA-Administrators
- Kontaktname des Rechners
- Anzahl der mit diesem Rechner verknüpften Tickets. Klicken Sie auf das Symbol , um die Tickets in einer Ticket-Tabelle anzuzeigen.
- Anzahl der mit diesem Rechner verknüpften Alarme. Klicken Sie auf das Symbol , um für den betreffenden Rechner die Seite **Alarmübersicht** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4112.htm)* zu öffnen.

`admin contact`, `contact name`, `contact phone` und `contact email` können auf der Seite "Agent > **Profil bearbeiten** *(siehe 73)*" festgelegt werden. Alle anderen Felder werden in Audits erfasst und auf den Seiten "Agent > **Agentstatus** *(siehe 32)*" oder "Audit > **Rechnerübersicht** *(siehe 151)*" angezeigt.

Benachrichtigungsbalken-Einstellungen

Rechts außen neben dem Benachrichtigungsbalken bietet das Zahnradsymbol Zugriff auf die **Benachrichtigungsbalken-Einstellungen**, mit denen der Berichtigungsbalken benutzerdefiniert angepasst werden kann. Dazu gehört:

- Auswahl unterschiedlicher Symbole für die verschiedenen Arten von Benachrichtigungen
- Auswahl das Systemwarnungen, die Sie erhalten möchten
- Auswahl der "Eindringlichkeit" der Benachrichtigung: im Hintergrund, subtil oder sehr deutlich.
- Verwendung des Trennbalkens zum Gruppieren von Symbolen
- Ausblenden von Benachrichtigungen, die keine Elemente aufweisen

Die einzelnen Benachrichtigungssymbole können durch Ziehen im Benachrichtigungsbalken einfach nach links oder rechts verschoben werden.

Navigation, linke Seite

Rechts außen neben dem Benachrichtigungsbalken bietet das Zahnradsymbol Zugriff zu den zwei Optionen für **Navigation, linke Seite**.

- **Shortcuts** – Wenn aktiviert, wird die Symbolleiste oberhalb des Navigationsfelds angezeigt.
- **Navigation durchsuchen** – Wenn aktiviert, wird oberhalb des Navigationsfelds ein Suchfeld angezeigt.

Meldungen

Derzeit werden im Benachrichtigungsbalken nur Meldungen angezeigt, die mithilfe des **Agent-Verfahren**-Befehls **SendAlert()** *(siehe 113)* generiert wurden. In zukünftigen Versionen werden weitere Arten von Meldungen unterstützt.

Toolbox



Die **Toolbox** stellt Benutzern einen gemeinsamen Bereich zur Verfügung, über den sie auf häufig verwendete Befehle und Funktionen zugreifen können. Die **Toolbox** kann von jedem Modul aus aufgerufen werden und bietet Benutzern einfachen Zugriff auf häufig verwendete Funktionen im VSA.

Anmerkungen

Klicken Sie auf das Symbol **Anmerkungen** , um das Fenster **Benutzeranmerkungen** *(siehe 14)*

einzublenden. Das Fenster **Benutzeranmerkungen** bietet einen Bereich, in dem Sie aufzeichnen bzw. abrufen können, welche früheren Benutzeraktionen auf einem Rechner durchgeführt wurden.

Status

Klicken Sie auf das Symbol **Status** , um das Fenster **Status-Monitor** *(siehe 13)* einzublenden. Der **Status-Monitor** überwacht kontinuierlich die ausgewählten Rechner und benachrichtigt Sie, wenn diese online oder offline gehen.

Hilfe

Klicken Sie auf das Symbol **Hilfe** , um kontextspezifische Hilfe für die derzeit ausgewählte Funktionsseite anzuzeigen.

Statusmonitor

Toolbox > Status

Der Status-Monitor überwacht kontinuierlich die ausgewählten Rechner und benachrichtigt Sie, wenn diese online oder offline gehen. Wenn jemand gegenwärtig bei einem Rechner angemeldet ist, zeigt der **Status-Monitor** den Benutzernamen (fettgedruckt) zusammen mit der IP-Adresse des Rechners an. Hauptrollenbenutzer können außerdem die Liste der angemeldeten VSA-Benutzer anzeigen.

Ton ausschalten

Ein eindeutiges akustisches Signal ertönt jedes Mal, wenn ein Rechner online bzw. offline geht oder wenn sich ein Benutzer an- bzw. abmeldet. Durch Aktivieren dieses Felds können Sie diese akustischen Signale ausschalten.

Bildwiederholfrequenz

Aktualisiert den Browser alle 30 Sekunden bzw. 1, 2 oder 5 Minuten. Bei jeder Browseraktualisierung wird der aktuelle Status von **Virtual System Administrator™** abgerufen. Um eine sofortige Aktualisierung zu erhalten, klicken Sie auf den Link **Aktualisieren**.

Eingeloggte Benutzer auflisten

Deaktivieren Sie dieses Feld, um die Liste der Benutzer auszublenden.

Hinweis: Diese Option steht nur Benutzern mit Masterrolle zur Verfügung.

Sortieren nach

Rechner können in einer der folgenden Anordnungen aufgelistet werden:

- **Connection Gateway** – Numerisch von links nach rechts, nach IP-Adresse. Am besten geeignet, um Rechner danach zu gruppieren, wie sie mit dem Netzwerk verbunden sind.
- **Gruppen-ID** – Alphabetisch nach Gruppen-ID.
- **Rechner-ID** – Alphabetisch nach Rechner-ID.

Offline-Rechner ausblenden

Deaktivieren Sie dieses Feld, um alle Rechner aufzulisten. Offline-Rechner sind durch ein grau abgeblendetes Symbol gekennzeichnet.

Administratoranmerkungen

Mithilfe von **Administratoranmerkungen** können Sie in der Systemdatenbank protokollieren, welche Aufgaben Sie mit einem Rechner oder einer Gruppe von Rechnern durchgeführt haben. Wenn Sie das nächste Mal auf ein Problem mit einem Rechner stoßen, können Sie die Anmerkungen überprüfen und nachsehen, welche Vorgänge andere VSA-Benutzer auf diesem Rechner durchgeführt haben. Das System versieht jede Administratoranmerkung mit einem Zeitstempel und ordnet die Anmerkung einem VSA-Benutzernamen zu. Öffnen Sie den Anmerkungseditor durch Klicken auf das Anmerkungen-Symbol in der **Toolbox** *(siehe 12)*, in **Live-Connect** *(siehe 393)*, in der **Rechnerübersicht** *(siehe 151)* oder in der **Schnellanzeige** *(siehe 17)*.

> **Hinweis:** Sie können **Administratoranmerkungen** unter "Infocenter > Reporting > Berichte > Protokolle - **Administratorhinweise** *(siehe 218)* ausdrucken.
>
> **Hinweis:** "Audit > **Dokumente** *(siehe 158)*" bietet eine andere Methode zur Dokumentation eines Rechners, und zwar durch Hochladen der Dokumentationsdateien eines bestimmten Rechners auf den Kaseya Server.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen. Aktivieren Sie dieses Feld vor den Rechnern, auf die Sie die Anmerkung anwenden möchten.

Zeit

Zeigt die Uhrzeit an, zu der die Anmerkung erstmals eingegeben wurde. Der Zeitstempel kann durch Klicken auf das Bearbeitungssymbol neben der Anmerkung, deren Zeitstempel Sie ändern möchten, bearbeitet werden.

Admin

Anmeldungsname des Benutzers, der die Anmerkung eingegeben hat. Falls ein anderer Benutzer die Anmerkung bearbeitet, wird dieses Feld mit dem Namen des neuen Benutzers aktualisiert.

Anmerkung löschen

Sie löschen die Anmerkung durch Klicken auf das nebenstehende Löschen-Symbol . Falls auf mehreren Rechnern die gleiche Anmerkung vom gleichen Benutzer und mit dem gleichen Zeitstempel eingegeben wurde, werden Sie vom System gefragt, ob Sie alle Vorkommnisse der Anmerkung löschen möchten.

Anmerkung bearbeiten

Sie ändern eine Anmerkung durch Klicken auf das nebenstehende Bearbeitungssymbol . Klicken Sie auf **Apply**, um die Änderungen einzuspeichern. Klicken Sie auf **Abbrechen**, um den Originaltext wiederherzustellen. Falls auf mehreren Rechnern die gleiche Anmerkung vom gleichen Benutzer und mit dem gleichen Zeitstempel eingegeben wurde, werden Sie vom System gefragt, ob Sie alle Vorkommnisse der Anmerkung ändern möchten.

Hinweis

Zeigt die vom Benutzer eingegebene Anmerkung für den ausgewählten Rechner an.

Anmerkungen pro Seite

Die Anzahl der Anmerkungen, die gleichzeitig angezeigt werden. Mögliche Auswahlen sind 10, 30 und

100.

Lesezeichen

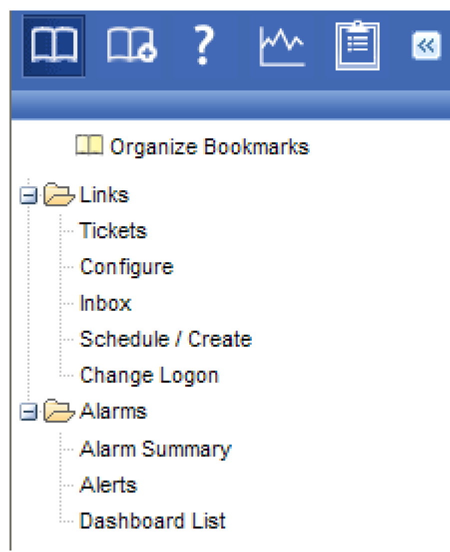


Sie können jedes beliebige Element im Navigationsfeld mit einem Lesezeichen versehen. Lesezeichen werden vom Benutzer definiert. Wenn Sie jeden Tag mit der gleichen Gruppe von Navigationselementen arbeiten, können Sie sich damit viele Navigationsklicks ersparen.

– Klicken Sie auf das Symbol **Lesezeichen hinzufügen**, um in Ihrer Liste von Lesezeichen ein Navigationselement hinzuzufügen.

– Klicken Sie auf das Symbol **Lesezeichen anzeigen**, um die Liste der gespeicherten Lesezeichen anzuzeigen.

– Klicken Sie auf das Symbol **Lesezeichen organisieren** in der Lesezeichenliste, um Lesezeichenordner zu erstellen und Ihre Lesezeichen zu organisieren.



Abmeldung

Klicken Sie auf den Link **Abmelden**, um den unautorisierten Zugriff auf den Server zu verhindern und zur Anmeldeseite zurückzukehren. Der Link **Abmelden** befindet sich in der oberen rechten Ecke des Fensters und kann von jeder Registerkarte und Funktion aufgerufen werden.

> **Hinweis:** Aus Sicherheitsgründen wird empfohlen, dass sich Benutzer abmelden und alle Browsersitzungen beenden, wenn sie keine Serveradministration durchführen.

Farbschema

System > Anpassen > Farbschema

Die Seite **Farbschema** legt die Farben fest, die von der VSA-Umgebung für den aktuellen Benutzer angezeigt werden. Die Auswahl des **Farbschemas** gilt für alle Benutzer in derselben **Partition** *(siehe 631)*.

So ändern Sie das Farbschema:

1. Wählen Sie im mittleren Fensterbereich ein Farbschema aus.
2. Klicken Sie auf die Schaltfläche **Schema konfigurieren**.

Agents

Die Verwaltung der Rechner über den VSA erfolgt durch Installieren eines Software-Clients auf einem verwalteten Rechner, der als ein **Agent** bezeichnet wird. Bei dem Agent handelt es sich um einen Systemdienst, bei dem der Benutzer nicht angemeldet sein muss, damit der Agent funktioniert, und der auch keinen Neustart erfordert, damit der Agent installiert werden kann. Der Agent ist konfigurierbar und kann für den Benutzer völlig unsichtbar sein. Der einzige Zweck des Agents ist es, die vom VSA-Benutzer angeforderten Aufgaben auszuführen. Nach der Installation:

- In der Systemablage des verwalteten Rechners wird ein Agent-Symbol, wie beispielsweise das Agent-Symbol angezeigt. Bei **Agent-Symbolen** *(siehe 24)* kann es sich um benutzerdefinierte Bilder handeln. Sie können jedoch auch ganz entfernt werden.
- Jedem installierten Agent wird eine eindeutige VSA **Rechner-ID/Gruppen-ID/Organisation-ID** *(siehe 626)* zugewiesen. Rechner-IDs können automatisch bei der Installation des Agents oder einzeln vor der Installation des Agents erstellt werden.
- Jeder installierte Agent verbraucht eine der verfügbaren Agent-Lizenzen, die vom Service-Provider erworben wurden.
- Agents werden in der Regel über Pakete installiert, die mit Agent > **Agents bereitstellen** *(siehe 40)* im VSA erstellt werden.
- Auf einem Rechner können **mehrere Agents** *(siehe 50)* installiert werden, die jeweils auf einen anderen Server verweisen.
- Neben jeder Rechner-ID im VSA wird ein **Check-in-Symbol** *(siehe 16)* angezeigt, das den Gesamtstatus des verwalteten Rechners angibt. Das Anmeldsymbol weist beispielsweise darauf hin, dass der Agent online und der Benutzer momentan angemeldet ist.
- Wenn Sie auf ein Anmeldesymbol klicken, wird eine einzelne Rechneroberfläche für den verwalteten Rechner namens **Live-Connect** *(siehe 17)* angezeigt. **Live-Connect** bietet sofortigen Zugriff auf umfassende Daten und Tools, die Sie für das Arbeiten auf diesem spezifischen Rechner benötigen.
- Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt. Über das Agent-Schnellansichtsfenster können Sie ein Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten.

Check-in-Symbole

Nachdem eine Rechner-ID erstellt wurde, wird neben jedem Rechner-ID-Konto im VSA ein Check-in-Symbol angezeigt. Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Klicken Sie auf ein Check-in-Symbol, um **Live-Connect** *(siehe 17)* zu öffnen. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet. Das Symbol zeigt eine Quickinfo mit dem Anmeldenamen an.

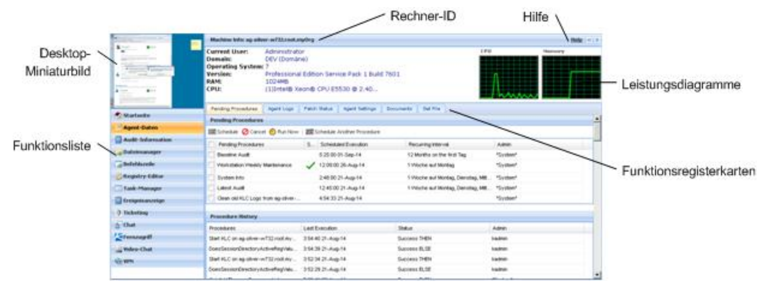
Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Live-Connect

Live Connect ist eine webbasierte, einzelne Rechneroberfläche. Sie können auf **Live Connect** durch Drücken der Strg-Taste und Klicken auf das Agent-Symbol oder durch Klicken auf die Schaltfläche **Live Connect** in der **Schnellansicht** *(siehe 17)* zugreifen. Mithilfe von **Live Connect** können Sie Aufgaben und Funktionen für jeweils einen verwalteten Rechner ausführen. Ein Menü von Eigenschaftenblättern in Form von Registerkarten ermöglicht den Zugriff auf verschiedene Kategorien von Informationen zu dem verwalteten Rechner.



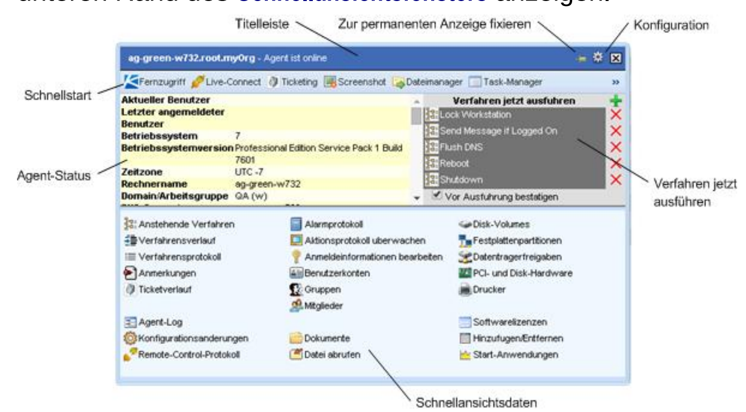
Je nach installierten Zusatzmodulen und dem Betriebssystem des Zielrechners werden weitere Menüelemente angezeigt.

Das gleiche **Live Connect**-Fenster wird auch angezeigt, wenn ein Benutzer des Rechners auf das Agent-Symbol in der Systemablage des verwalteten Rechners klickt. In diesem Fall gelten jedoch bestimmte Beschränkungen. Die Ansicht dieses Rechnerbenutzers von **Live Connect** wird als **Portalzugriff** bezeichnet.

> **Hinweis:** Weitere Informationen finden Sie unter "Remote-Control > **Live Connect** *(siehe 393)*".

Schnellanzeige

Wenn Sie den Cursor auf ein Check-in-Symbol bewegen, wird sofort das **Agent-Schnellansichtsfenster** geöffnet. Im **Agent-Schnellansichtsfenster** können Sie Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten. Mithilfe von **Agent-Zeichen** *(siehe 18)* können Sie Text für **besondere Anweisungen** am unteren Rand des **Schnellansichtsfensters** anzeigen.



Screenshot

Diese Funktion steht ausschließlich im Fenster **Schnellanzeige** zur Verfügung. Klicken Sie auf die Schaltfläche **Screenshot**, um ein Bildschirmabbild des aktuellen Desktops anzufertigen. Die gespeicherten Bilder öffnen Sie über das Ordnersymbol **Datei abrufen** im selben Fenster (**Schnellanzeige**).

Desktop aufzeichnen

Gilt nur für Rechner, denen der Remote-Control-Typ WinVNC zugewiesen wurde. Die Schaltfläche **Desktop aufzeichnen** zeichnet den Desktop auf, ohne eine Remote-Control-Sitzung zu starten.

Agent-Zeichen

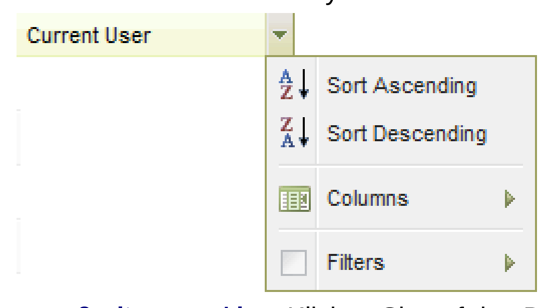
Fügen Sie *Zeichen* zur unteren rechten Ecke des Agentstatussymbols hinzu, wie . Diese Zeichen werden überall angezeigt, wo das Agent-Symbol in der Benutzeroberfläche erscheint. Sie können beispielsweise einen Rechner mit einem -Zeichen versehen, um anzugeben, dass der Kunde einen Telefonanruf bekommen muss, bevor jemand an diesem Rechner arbeitet. Sie können einen Server auch mit einem -Zeichen markieren, damit dieser erst nach Betriebsschluss verwendet wird.

Wählen Sie auf der Seite Agent > **Profil bearbeiten** *(siehe 73)* mindestens einen Rechner aus. Klicken Sie anschließend auf den Link **Symbol-Abzeichen** oben auf der Seite und wählen Sie eines der verfügbaren Zeichen aus. Sie können eine Textnachricht mit **speziellen Anweisungen** für jedes Zeichen definieren. Klicken Sie auf die Schaltfläche **Aktualisieren**, um das Zeichen ausgewählten Rechnern zuzuweisen.

Wenn Sie den Cursor über ein Agent-Statussymbol mit einem Zeichen bewegen, wird das Fenster **Schnellansicht** *(siehe 17)* im Text mit den **speziellen Anweisungen** unten im Fenster angezeigt.

Optionen für Datentabellenspalten

Für Datentabellen in Kaseya 2 stehen üblicherweise die folgenden Spaltenoptionen zur Verfügung.



- **Spaltenauswahl** – Klicken Sie auf den Dropdown-Pfeil in einer beliebigen Spaltenüberschrift und anschließend auf **Spalten**, um die Spalten anzugeben, die in der Tabelle angezeigt werden sollen. Klicken Sie auf die Symbole für Aufsteigende Reihenfolge oder Absteigende Reihenfolge , um die Tabelle nach der ausgewählten Spaltenüberschrift zu sortieren.
- **Spaltensortierung** – Klicken Sie auf die Symbole für aufsteigende Reihenfolge oder absteigende Reihenfolge , um die Tabelle nach der ausgewählten Spaltenüberschrift zu sortieren.
- **Spaltenfilter** – Klicken Sie auf den Dropdown-Pfeil in der Spalte, um einen Filterwert für diese Spalte einzugeben. Geben Sie zum Beispiel `NS` ein, um alle Zeilen in dieser Spalte zu finden, die mit `NS` beginnen. Geben Sie `NS%2` ein, um alle Zeilen in dieser Spalte zu finden, die mit **NS** beginnen und mit `2` enden. Wunschgemäß können Sie nach mehreren Spaltenfiltern filtern.

- **Flexible Spaltenbreiten** – Erweitern oder reduzieren Sie die Breite jeder Spalte durch Ziehen der Spaltenüberschriftbegrenzungen nach rechts oder nach links.

Weiterführende Themen

Für die ersten Schritte bei der Implementierung von **Virtual System Administrator™** stehen PDF-Dokumente zur Verfügung. Diese können unter dem **ersten Thema in der VSA-Online-Hilfe** *(http://help.kaseya.com/webhelp/DE/VSA/7000000)* heruntergeladen werden.

Falls Sie mit **Virtual System Administrator™** noch nicht vertraut sind, empfehlen wir die folgenden Schnellstart-Handbücher:

1. Erste Schritte
2. Benutzer-Administration
3. Konfiguration und Bereitstellung von Agents
4. Remote-Control-Tools
5. Kontrollkonfiguration
6. Benutzerdefinierte Berichte

Die folgenden Ressourcen stehen ebenfalls zur Verfügung.

Kaseya University

Im **Kaseya University** *(http://university.kaseya.com)* finden Sie verschiedenste Schulungsangebote.

Kapitel 3

Agent

In diesem Kapitel

Agent-Übersicht

Agent

Mithilfe der Funktionen im Modul **Agent** können Benutzer Rechner-IDs erstellen, bearbeiten und löschen, das Aussehen des Agent-Symbols auf dem Rechner in der **Systemablage** *(on seite 631)* ändern, die Häufigkeit der Agent-Anmeldung steuern und die Version der auf verwalteten Rechnern gespeicherten Agent-Software aktualisieren.

> **Hinweis:** Wenn Sie sich mit der Agent-Installation noch nicht auskennen, beziehen Sie sich auf die Schnellstartanleitung Agent-Konfiguration und Verteilung.

Funktionen	Beschreibung
Agentstatus *(siehe 32)*	Zeigt aktive Benutzerkonten, IP-Adressen und die letzten Check-in-Zeiten an.
Agentprotokolle *(siehe 35)*	Zeigt die folgenden Protokolle an: • Agent-System- und Fehlermeldungen • Ausführung der Agent-Verfahren, ob erfolgreich oder fehlgeschlagen. • Von einem Benutzer vorgenommene Konfigurationsänderungen. • Senden/Empfangen von Daten für Anwendungen, die auf das Netzwerk zugreifen. • Anwendungs-, System- und Sicherheitsdaten im Ereignisprotokoll, die vom verwalteten Rechner erfasst wurden. • Alarmprotokoll • Fernsteuerungsprotokoll • Protokollüberwachung
Protokollhistorie *(siehe 36)*	Gibt an, wie lange die Protokolldaten gespeichert werden sollen.
Ereignisprotokolleinstellungen *(siehe 36)*	Gibt die in Ereignisprotokollen enthaltenen Protokolltypen und -kategorien an.
Agents verteilen *(siehe 40)*	Erstellt Agent-Installationspakete zum Installieren von Agents auf mehreren Rechnern.
Erstellen *(siehe 55)*	Erstellt Rechner-ID-Konten und/oder Installationspakete zum Installieren von Agents auf einzelnen Rechnern.
Löschen *(siehe 58)*	Löscht Rechner-ID-Konten.
Umbenennen *(siehe 60)*	Benennt vorhandene Rechner-ID-Konten um.
Gruppe ändern *(siehe 62)*	Weist Rechner einer anderen Rechnergruppe oder Untergruppe zu.
Einstellungen kopieren *(siehe 62)*	Kopiert Einstellungen von einem Rechnerkonto auf andere Rechnerkonten per Massenkopie.
Import/Export *(siehe 64)*	Importiert und exportiert Agent-Einstellungen, einschließlich geplanter Agent-Verfahren, zugewiesener Monitor-Sets und Ereignissätze als XML-Dateien.
Aussetzen *(siehe 65)*	Setzt alle Agent-Operationen, z. B. Agent-Verfahren, Monitoring und Patching aus, ohne die Einstellungen des

	Agents zu ändern.
Agent-Menü *(siehe 66)*	Passt das Agent-Menü auf verwalteten Rechnern an.
Check-in-Kontrolle *(siehe 68)*	Kontrolliert, wie oft Agents sich auf Agent-Rechnern anmelden.
Arbeitsverzeichnis *(siehe 72)*	Stellt einen Pfad zum Verzeichnis her, das vom Agent zum Speichern der Arbeitsdateien verwendet wird.
Profil bearbeiten *(siehe 73)*	Bearbeitet Rechnerkontodaten.
Portalzugriff *(siehe 75)*	Richtet Konten ein, um Rechnerbenutzern Fernzugriff auf ihre eigenen Rechner zu gestatten.
Anmeldedaten eingeben *(siehe 77)*	Stellt Anmeldedaten ein, die der Agent im Patch-Management, dem Verfahrensbefehl "Anmeldedaten verwenden", Endpoint Security und Desktop Management verwendet.
LAN-Cache *(siehe 78)*	Designiert einen Rechner so, dass er als Dateiquelle für andere Rechner auf dem gleichen LAN agiert.
LAN-Cache zuweisen *(siehe 81)*	Weist Rechner einem ausgewählten LAN-Cache-Rechner zu bzw. entfernt sie daraus.
Agent aktualisieren *(siehe 81)*	Aktualisiert die Agent-Software auf verwalteten Rechnern.
Dateizugriff *(siehe 83)*	Verhindert unberechtigten Zugriff auf Dateien auf verwalteten Rechnern durch Rogue-Anwendungen oder Benutzer.
Netzwerkzugriff *(siehe 84)*	Ermöglicht Ihnen, den Netzwerkzugriff auf Anwendungsbasis zu gestatten oder abzulehnen.
Anwendungsblocker *(siehe 88)*	Anwendungsblocker verhindert, dass beliebige Anwendungen auf einem verwalteten Rechner ausgeführt werden.

Agents

Die Verwaltung der Rechner über den VSA erfolgt durch Installieren eines Software-Clients auf einem verwalteten Rechner, der als ein **Agent** bezeichnet wird. Bei dem Agent handelt es sich um einen Systemdienst, bei dem der Benutzer nicht angemeldet sein muss, damit der Agent funktioniert, und der auch keinen Neustart erfordert, damit der Agent installiert werden kann. Der Agent ist konfigurierbar und kann für den Benutzer völlig unsichtbar sein. Der einzige Zweck des Agents ist es, die vom VSA-Benutzer angeforderten Aufgaben auszuführen. Nach der Installation:

- In der Systemablage des verwalteten Rechners wird ein Agent-Symbol, wie beispielsweise das Agent-Symbol angezeigt. Bei **Agent-Symbolen** *(siehe 24)* kann es sich um benutzerdefinierte Bilder handeln. Sie können jedoch auch ganz entfernt werden.
- Jedem installierten Agent wird eine eindeutige VSA **Rechner-ID/Gruppen-ID/Organisation-ID** *(siehe 626)* zugewiesen. Rechner-IDs können automatisch bei der Installation des Agents oder einzeln vor der Installation des Agents erstellt werden.
- Jeder installierte Agent verbraucht eine der verfügbaren Agent-Lizenzen, die vom Service-Provider erworben wurden.
- Agents werden in der Regel über Pakete installiert, die mit Agent > **Agents bereitstellen** *(siehe 40)* im VSA erstellt werden.
- Auf einem Rechner können **mehrere Agents** *(siehe 50)* installiert werden, die jeweils auf einen anderen Server verweisen.

- Neben jeder Rechner-ID im VSA wird ein **Check-in-Symbol** *(siehe 16)* angezeigt, das den Gesamtstatus des verwalteten Rechners angibt. Das Anmeldsymbol weist beispielsweise darauf hin, dass der Agent online und der Benutzer momentan angemeldet ist.
- Wenn Sie auf ein Anmeldesymbol klicken, wird eine einzelne Rechneroberfläche für den verwalteten Rechner namens **Live-Connect** *(siehe 17)* angezeigt. **Live-Connect** bietet sofortigen Zugriff auf umfassende Daten und Tools, die Sie für das Arbeiten auf diesem spezifischen Rechner benötigen.
- Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt. Über das Agent-Schnellansichtsfenster können Sie ein Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten.

Agent-Symbole

Nachdem der Agent auf einem Rechner installiert wurde, wird er durch ein Symbol in der Systemablage des Rechners angezeigt. Dieses Symbol stellt die Schnittstelle des Rechnerbenutzers zum Agent dar. Das Symbol kann auf Wunsch des VSA-Benutzers über die Seite Agent > **Agent-Menü** *(siehe 66)* deaktiviert werden.

> **Hinweis:** Über System > Site-Anpassung können Sie Agent-Symbole vollständig anpassen. Siehe **Benutzerdefinierte Agent-Symbole erstellen** *(siehe 450)*. Dies gilt auch für eindeutige Symbole für Apple- und Linux-Rechner.

Hintergrund des Agent-Symbols ist blau

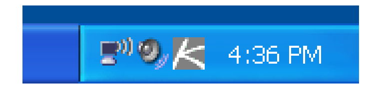
Wenn der Agent ausgeführt wird und **erfolgreich in den VSA eincheckt**, wird der Hintergrund des Agent-Symbols **blau** dargestellt.



> **Hinweis:** Durch Doppelklicken auf das Agent-Symbol wird die **Willkommensseite für den Portal-Zugang** *(siehe 625)* angezeigt.

Hintergrund des Agent-Symbols ist grau

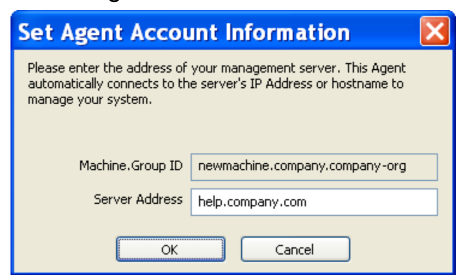
Ein ausgeführter Agent, der **nicht** in den VSA einchecken kann, wird als **graues Symbol** dargestellt. Dies zeigt an, dass entweder die Netzwerkverbindung ausgefallen ist oder der Agent an die falsche Adresse für den VSA verwiesen wird.



Bei einem grauen Agent-Symbol überprüfen Sie Folgendes:

1. Vergewissern Sie sich, dass dieser Rechner über Internetzugang verfügt.
2. Prüfen Sie, ob eine Firewall den **ausgehenden** Port blockiert, der vom Agent für die Verbindung mit dem VSA verwendet wird. Der Standard-Port ist 5721.
3. Vergewissern Sie sich, dass die Einstellungen für die **Check-in-Kontrolle** *(siehe 68)* für dieses Rechnerkonto korrekt sind.

4. Stellen Sie die VSA-Server-Adresse im Agent manuell ein, indem Sie mit der rechten Maustaste auf das Agentmenü klicken, **Konto einrichten...** auswählen und die richtige Adresse in das Formular eingeben.



Hintergrund des Agent-Symbols ist rot

Das Agent-Symbol wechselt zu **rot**, wenn ein Rechnerbenutzer die Fernsteuerung manuell deaktiviert. VSA-Benutzer verhindern die Fernsteuerung ihres Rechners durch andere Personen, indem sie mit der rechten Maustaste auf das Agent-Menü klicken und **Fernsteuerung deaktivieren** auswählen.



Hintergrund des Agent-Symbols blinkt abwechselnd weiß und blau

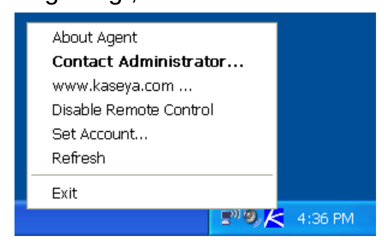
Das Agent-Symbol **blinkt** abwechselnd mit einem weißen Hintergrund und seinem normalen Hintergrund, wenn eine *Nachricht darauf wartet* gelesen zu werden. Die Nachricht wird durch Klicken auf das Symbol angezeigt.



Hinweis: Eine Erläuterung dazu, wie das Senden von Nachrichten eingerichtet wird, finden Sie unter Fernsteuerung > **Nachricht senden** *(siehe 391)*.

Optionen im Agent-Menü

Durch das Klicken mit der rechten Maustaste auf das Agent-Symbol wird ein Menü mit Optionen angezeigt, die dem Rechnerbenutzer zur Verfügung stehen.



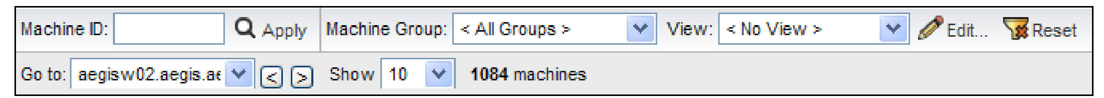
Hinweis: Wie diese Optionen aktiviert oder deaktiviert werden, wird unter Agent > **Agent-Menü** *(siehe 66)* beschrieben.

Agent-Menü deaktivieren

VSA-Benutzer können das **Agent-Menü deaktivieren** *(siehe 66)* und das Symbol vom Desktop des Rechners entfernen.



Rechner-ID-/Rechnergruppen-Filter



Der Rechner-ID-/Rechnergruppen-ID-Filter steht auf allen Registerkarten und in allen Funktionen zur Verfügung. Mit seiner Hilfe können *Sie* anstelle eines Administrators die auf *allen* Funktionsseiten angezeigten Rechner beschränken. Über das Fenster **Definitionen anzeigen** können Sie einen Rechner-ID-/Rechnergruppen-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern. Nachdem Sie die Filterparameter angegeben haben, klicken Sie auf die Schaltfläche **Anwenden**, um die Filtereinstellungen auf *alle* Funktionsseiten anzuwenden. Der Rechner-ID-/Rechnergruppen-ID-Filter zeigt standardmäßig alle Rechner-IDs in `<All Groups>` an, die vom gegenwärtig angemeldeten VSA-Benutzer verwaltet werden.

> **Hinweis:** Selbst wenn ein VSA-Benutzer `<All Groups>` auswählt, werden nur Gruppen angezeigt, auf die dem VSA-Benutzer über System > Benutzersicherheit > **Scopes** *(siehe 419)* Zugriff gewährt wurde.

- **Rechner-ID** – Beschränkt die Anzeige von Daten auf *allen* Funktionsseiten nach Rechner-ID-Zeichenfolge. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Beispiel: Durch die Eingabe der Zeichenfolge `ABC*` wird die Anzeige der Rechner-IDs auf allen Funktionsseiten auf Rechner-IDs beschränkt, die mit den Buchstaben `ABC` beginnen.

  Filtert die Anzeige von Rechnern nach Rechner-ID. Geben Sie den *Anfang* einer Zeichenfolge ein, um alle Rechner-IDs anzuzeigen, die mit dieser Zeichenfolge übereinstimmen. Fügen Sie ein Sternchen am Anfang einer Zeichenfolge ein, um alle Geräte zu finden, die mit der Zeichenfolge an einer beliebigen Stelle in der Rechner-ID übereinstimmen. Durch Eingabe der Zeichenfolge `*ABC` werden beispielsweise alle Rechner-IDs gesucht, die ABC an einer beliebigen Stelle in der Rechner-ID haben.
- **Anwenden** – Klicken Sie auf die Schaltfläche **Anwenden**, um die Filtereinstellungen auf alle Funktionsseiten anzuwenden.
- **Rechnergruppe** – Beschränkt die Anzeige von Daten auf allen Funktionsseiten nach **Gruppen-ID oder Organisation** *(siehe 626)*. Eine Organisation mit nur *einer Rechnergruppe* zeigt nur die Rechnergruppe in der Drop-Down-Liste **Rechergruppe** an, nicht die Organisation. Organisationen mit *mehreren Rechnergruppen* zeigen die Organisation und alle Rechnergruppe für diese Organisation an. Dadurch kann die Organisation optional ausgewählt werden, um alle Rechnergruppen mit einzuschließen.
- **Anzeigen** – Ändern Sie die Ansichten, indem Sie eine andere Ansichtsdefinition auswählen. Über das Fenster **Definitionen anzeigen** können Sie einen Rechner-ID-/Rechnergruppen-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern.
- **Bearbeiten...** – Klicken Sie auf diese Option, um die Seite **Ansichtsdefinitionen** *(siehe 27)* anzuzeigen.
- **Zurücksetzen** – Löscht alle Filterungen.
- **Gehe zu** – Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.
- **Anzeigen** – Wählen Sie die Anzahl der Rechner-IDs aus, die auf jeder Seite angezeigt werden.
- **(Rechnerzahl)** – Zeigt die Rechnerzahl basierend auf den Filtereinstellungen an.

Ansichtdefinitionen

Rechner-ID-/Gruppen-ID-Filter > Bearbeiten...

Über das Fenster **Definitionen anzeigen** können Sie einen Rechner-ID-/Rechnergruppen-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern. Sie können mehrere Ansichten erstellen und benennen. Die Ansichtsfilterung wird auf *alle* Funktionsseiten angewendet, indem Sie eine **Ansicht** aus der Dropdown-Liste im Feld **Rechner-ID/Rechnergruppenfilter** *(siehe 26)* auswählen und auf das Symbol **Anwenden** klicken. Optionen werden nach Abschnitten organisiert, die nach Bedarf erweitert und reduziert werden können. Wenn eine Option eingestellt ist, bleibt der Abschnitt erweitert.

Kopfzeilenoptionen

- **Speichern** – Speichern Sie die ausgewählte Ansicht.
- **Speichern unter** – Speichern Sie die ausgewählte Ansicht unter einem neuen Namen.
- **Löschen** – Löschen Sie die ausgewählte Ansicht.
- **Ansicht auswählen** – Wählen Sie eine Ansicht aus.
- **Titel bearbeiten** – Bearbeiten Sie den Titel einer Ansicht.
- **Freigabe....** – Sie können eine Ansicht mit ausgewählten VSA-Benutzern und Benutzerrollen **gemeinsam nutzen** *(siehe 421)* oder für alle VSA-Benutzer und Benutzerrollen freigeben.

So erstellen oder bearbeiten Sie eine neue Ansicht:

1. Klicken Sie auf die Schaltfläche **Bearbeiten...** rechts neben der Dropdown-Liste **Ansicht** im Feld für den Rechner-ID-/Gruppen-ID-Filter, um den Editor **Ansichtdefinitionen** zu öffnen.
2. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie einen Namen für die neue Ansicht ein.
3. Geben Sie die gewünschten Filterspezifikationen ein.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Rechnerfilter

- **Rechner-ID einstellen** – Durch Aktivieren dieses Kontrollkästchens wird jeder Wert, der für das Feld **Rechner-ID** unter Rechner-ID-/Gruppen-ID-Filter eingestellt wurde, durch den hier eingegebenen Wert überschrieben. Das Feld Rechner-ID ist auf der Filterleiste Rechner-ID-/Gruppen-ID deaktiviert, um unabsichtliche Änderungen zu verhindern, wenn eine Ansicht angezeigt wird, bei der **Rechner-ID einrichten** ausgewählt ist.
- **Gruppen-ID einstellen** – Durch Aktivieren dieses Kontrollkästchens wird der **Gruppen-ID**-Filter im Feld für den Rechner-ID-/Gruppen-ID-Filter durch den hier eingegebenen Wert überschrieben. Das Feld Gruppen-ID ist auf der Filterleiste Rechner-ID-/Gruppen-ID deaktiviert, um unabsichtliche Änderungen zu verhindern, wenn eine Ansicht angezeigt wird, bei der **Gruppen-ID einstellen** ausgewählt ist.
- **Nur ausgewählte Rechner-IDs anzeigen** – Speichern Sie eine Ansicht zuerst, bevor Sie mit dieser Option Rechner-IDs auswählen. Sobald eine Ansicht gespeichert wurde, wird rechts von dieser Option ein Link **<N> Rechner ausgewählt** angezeigt. Klicken Sie auf diesen Link, um das Fenster **Sammlung definieren** anzuzeigen, in dem Sie mithilfe einer freien **Sammlung** *(siehe 628)* von Rechner-IDs eine Ansicht erstellen können.

Rechnerstatus

- **Rechner zeigen, die in den letzen N Perioden online waren/nicht online waren/niemals online waren** – Aktivieren Sie dieses Kontrollkästchen, um diejenigen Rechner aufzulisten, deren Agents innerhalb des angegebenen Zeitraums am Kaseya Server angemeldet oder nicht angemeldet waren. Verwenden Sie die Option **nie**, um **Rechner-ID-Vorlagen** *(siehe 627)*konten zu filtern, da diese Konten sich nie anmelden.
- **Rechner zeigen, die ausgesetzt/nicht ausgesetzt sind** – Aktivieren Sie dieses Kontrollkästchen, um ausgesetzte oder nicht ausgesetzte Rechner aufzulisten.

- **Rechner zeigen, die in den letzten N Periode neu gestartet/nicht neu gestartet wurden** – Aktivieren Sie dieses Kontrollkästchen, um Rechner aufzulisten, die während des angegebenen Zeitraums keinen Neustart ausgeführt haben.
- **Rechner mit dem Anmeldestatus** – Aktivieren Sie dieses Kontrollkästchen, um Rechner mit dem ausgewählten Status der **Anmeldedaten** *(siehe 614)* aufzulisten.
- **Connection Gateway-Filter** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Connection-Gateway mit dem angegebenen Filter übereinstimmt. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Beispielsweise entspricht `66.221.11.*` allen Connection-Gateway-Adressen von `66.221.11.1` bis `66.221.11.254`.
- **IP-Adressenfilter** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren IP-Adresse mit dem angegebenen Filter übereinstimmt. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Beispielsweise entspricht `66.221.11.*` allen IP-Adressen von `66.221.11.1` bis `66.221.11.254`.

Betriebssystem-Info

- **BS-Typ** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner aufzulisten, die nach dem letzten Audit das ausgewählte Betriebssystem haben.
- **BS-Version** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner aufzulisten, die nach dem letzten Audit die Betriebssystemzeichenfolge haben. Mit diesem Filter können Sie Rechner nach **Service Pack** identifizieren.

Skripting

- **Mit geplantem/nicht geplantem Agent-Verfahren** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, für die eine Ausführung des angegebenen Agen-Verfahrens geplant oder nicht geplant ist.

> **Hinweis:** Klicken Sie auf den Link **Agent-Verfahren auswählen**, um das Agent-Verfahren namentlich zu bezeichnen.

- **Letzter Ausführungsstatus erfolgreich/fehlgeschlagen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen das ausgewählte Agent-Verfahren bereits ausgeführt wurde. Wählen Sie das entsprechende Optionsfeld, um Rechner aufzulisten, auf denen das Agent-Verfahren erfolgreich ausgeführt wurde oder fehlschlug.
- **Agent-Verfahren wurde in den letzten N Tagen ausgeführt/nicht ausgeführt** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen das Agent-Verfahren während des angegebenen Zeitraums nicht ausgeführt wurde.

Anwendungen

- **Enthält Anwendung/Anwendung fehlt** – Aktivieren Sie dieses Kontrollkästchen, um unter Verwendung des angegebenen Filters nur die Rechner aufzulisten, auf denen eine Anwendung installiert oder nicht installiert ist. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Versionszeichenfolge ist > < = N** – Aktivieren Sie dieses Kontrollkästchen, um den Anwendungsfilter durch eine Versionsnummer größer als, kleiner als oder gleich einem angegebenen Wert noch weiter zu verfeinern.
- **Rechner mit folgendem installierten Modul anzeigen**
  - **Anti-Malware**
  - **Anti-Virus**

Zusatzmodule

- Filtern Sie Rechner basierend darauf, ob eine Client-Software für ausgewählte Zusatzmodule installiert ist.

Bezeichnung

- **Rechner mit allen oder einem beliebigen der folgenden Zeichen anzeigen** – Filtert Rechner über **alle** oder **beliebige** ausgewählte Zeichen.
- Eine Reihe von Schlüsseln in der lokalen Registrierung eines Rechners wird überprüft, um zu identifizieren, ob der Rechner als bestimmter Rechnertyp "gekennzeichnet" werden kann. Beispiele für Zeichen umfassen: `DNS Server`, `Domain Controller`, `POP3 Server`, `SMTP Server` und `SQL Server`. Die Kennzeichnung erfolgt automatisch. Jeder Agent-Rechner wird periodisch (in der Regel einmal pro Stunde) auf Konfigurationsänderungen überprüft, die die Kennzeichnung des Rechners beeinflussen könnten.

Patch-Verwaltung

- **Mitglieder der Patch-Richtlinie ein-/ausblenden** – Durch Aktivieren dieses Kontrollkästchens gemeinsam mit den Filtern Rechner-ID- und Gruppen-ID werden nur bestimmte Rechner aufgelistet, die zu einer spezifischen **Patch-Richtlinie** *(siehe 624)* (**Einblenden**) oder nicht (**Ausblenden**) gehören.
- **Rechner ohne Patch-Scanergebnisse (nicht gescannt)** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, die nicht auf fehlende Patches gescannt wurden.
- **Rechner, auf denen mehr als oder gleich N Patches fehlen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen eine angegebene Anzahl von Microsoft-Patches *fehlt*.
- **Patch-Richtlinie verwenden** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen eine angegebene Anzahl von *bestätigten fehlenden* Microsoft-Patches fehlen.
- **Patch-Scan geplant/nicht geplant** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, auf denen ein Patch geplant ist oder nicht.
- **Letzter Ausführungsstatus erfolgreich/fehlgeschlagen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Patch-Scan erfolgreich war oder fehlschlug.
- **Patch-Scan wurde in den letzten <N> <Perioden> ausgeführt / nicht ausgeführt** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Patch-Scan innerhalb eines angegebenen Zeitraums ausgeführt oder nicht ausgeführt wurden.
- **Rechner mit 'Neustart anstehend' für Patch-Installationen** – Aktivieren Sie dieses Kontrollkästchen, um Rechner aufzulisten, auf denen ein Neustart für Patch-Installationen ansteht.
- **Rechner mit Patch-Testergebnissen** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit dem ausgewählten Patch-Testergebnis aufzulisten.
- **Rechner mit automatischer Patch-Aktualisierungskonfiguration** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit der ausgewählten Konfiguration Automatische Aktualisierung aufzulisten.
- **Rechner mit Konfiguration für Patch-Neustartaktion** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit der ausgewählten Konfiguration für einen Neutstart aufzulisten.
- **Rechner mit Patch-Dateiquellenkonfiguration** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit der ausgewählten Konfiguration für eine Patch-Dateiquelle aufzulisten.
- **Auf Rechnern fehlt ein spezifisches Patch (KB-Artikel-ID verwenden – nur Ziffern)** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner aufzulisten, bei denen ein spezifisches Patch fehlt.
- **Rechner mit installiertem Patch (KB-Artikel-ID verwenden – nur Ziffern)** – Aktivieren Sie dieses Kontrollkästchen, um nur die Rechner mit einem installierten Patch, das von KB-Artikel identifiziert wurde, aufzulisten.
- **Als Dateifreigabe verwendete Rechner** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, die als Dateifreigabe mit Dateiquelle konfiguriert wurden.
- **Rechner mit Dateifreigabe auf ausgewähltem Rechner** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit Dateifreigabe, die mit Dateiquelle konfiguriert wurde, auszuwählen.

- **Rechner mit Patch-Scan-Quelle auf online festgelegt, Offline-Scan wurde jedoch zuletzt ausgeführt** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, deren Standard-Scan-Quelle auf online festgelegt ist, die jedoch zuletzt einen Offline-Scan ausgeführt haben.
- **Standard-Patch-Scan-Quelle Offline/Online.** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner mit einer Offline- oder Online-Standard-Patch-Scan-Quelle aufzulisten.
- **Automatische Windows-Aktualisierung aktiviert/deaktiviert** – Aktivieren Sie dieses Kontrollkästchen, um nur Rechner aufzulisten, bei denen die automatische Windows-Aktualisierung aktiviert/deaktiviert ist.

Monitoring

- **Nur Rechner mit zugeordneten Monitor-Sets anzeigen <Monitor-Set auswählen>** – Wählen Sie diese Option, um alle Rechner, denen dieses Monitor-Set zugeordnet ist, aufzulisten.
- **Nur Rechner mit zugeordneten Monitor-Sets anzeigen <SNMP-Set auswählen>** – Wählen Sie diese Option, um alle Rechner, denen dieses Monitor-Set zugeordnet ist, aufzulisten.

Erweiterte Filterung

- **Erweiterter Datenfilter für Agents** – Aktivieren Sie dieses Kontrollkästchen und klicken Sie auf die Schaltfläche **Filter definieren...**, um die Ansicht mithilfe von **Filter-Gesamttabelle** *(siehe 30)* noch weiter zu verfeinern.

  > **Warnung:** Sie müssen ein **Leerzeichen** eingeben, um den Operator in einem Filtereintrag von den Daten zu trennen. Der Filtereintrag `>= 500` enthält beispielsweise ein Leerzeichen genau nach dem Gleich-Zeichen.

Zusammengeführte Tabelle filtern

Rechner-ID-/Gruppen-ID-Filter > Bearbeiten... > Filter definieren...

Filter Gesamttabelle führt mehr als 75 Attribute für Agents und verwaltete Rechner auf, mit deren Hilfe eine Ansichtsdefinition unter Verwendung der Option **Erweiterte Filterung** *(siehe 30)* noch weiter verfeinert werden kann.

> **Hinweis: Kollektionen** *(siehe 628)* stellen eine alternative Methode zur Auswahl von Rechner-IDs für eine **Ansichtsdefinition** *(siehe 27)* dar. Dabei kommt es nicht darauf an, ob sie irgendwelche Attribute gemeinsam nutzen.

Benutzerdefinierte Attribute

Über die Seite Audit > **Systeminformation** *(siehe 154)* können Sie benutzerspezifische Attribute für **Filter Gesamttabelle** hinzufügen. Erstellen Sie dann Ansichtdefinitionen, die Rechner-IDs auswählen, die auf diesen benutzerdefinierten Attributen basieren.

Erweiterte Filterung

Erweiterte Filterung lässt Sie komplexe Suchvorgänge erstellen, um Daten auf nur die von Ihnen gewünschten Werte zu beschränken. Geben Sie Filterzeichenfolgen in dieselben Bearbeitungsfelder ein, in die Sie Filtertext eingeben.

> **Warnung:** Sie müssen ein **Leerzeichen** eingeben, um den Operator in einem Filtereintrag von den Daten zu trennen. Der Filtereintrag `>= 500` enthält beispielsweise ein Leerzeichen genau nach dem Gleich-Zeichen.

Erweiterte Filterung unterstützt die folgenden Operationen:

Leerzeichen

Schließen Sie die Zeichenfolge in Anführungszeichen ein, um darin nach Leerzeichen zu suchen.

Zum Beispiel: `"Microsoft Office*"` oder `"* Adobe *"`

Verschachtelte Operatoren

Alle Gleichungen werden von links nach rechts verarbeitet. Mit Klammern kann diese Standardeinstellung außer Kraft gesetzt werden.

Zum Beispiel: `(("* adobe " OR *a*) AND *c*) OR NOT *d* AND < m`

AND

Mit dem logischen Operator AND können Sie nach Daten suchen, die mehrere Werte enthalten müssen, aber an verschiedenen Stellen in der Zeichenfolge erscheinen können.

Zum Beispiel: `Microsoft* AND *Office*` gibt alle Elemente zurück, die sowohl Microsoft als auch Office in einer beliebigen Reihenfolge enthalten.

oder

Verwenden Sie den logischen Operator OR für die Suche nach Daten, die zwar mehrere Werte enthalten können, aber zumindest einen Wert enthalten müssen.

Zum Beispiel: `*Microsoft* OR *MS*` gibt alle Elemente zurück, die entweder Microsoft oder MS in beliebiger Reihenfolge enthalten.

NOT

Suchen Sie nach einer Zeichenfolge, die die Übereinstimmungsdaten nicht enthält.

Zum Beispiel: `NOT *Microsoft*` gibt alle Nicht-Microsoft-Anwendungen zurück.

Zum Beispiel: `NOT *Windows* AND NOT *update*` gibt alle Elemente zurück, die nicht entweder die Zeichenfolgen `Windows` oder `update` enthalten.

<, <= (Kleiner als oder kleiner als oder gleich)

Führt einen Zeichenfolgenvergleich aus, um alle Daten zurückzugeben, deren Wert weniger als der eingegebene Wert ist.

Zum Beispiel: `< G*` gibt alle Anwendungen aus, die mit einem Buchstaben kleiner als `G` beginnen.

Zum Beispiel: `< 3` gibt die Werte `2`, `21` und `287` zurück.

> **Hinweis:** Es kann auch nach Datumsangaben gesucht werden, aber dies muss im folgenden Format erfolgen: `YYYYMMDD HH:MM:SS` wobei `YYYY` das Jahr in 4-stelliger Schreibweise, `MM` den Monat in 2-stelliger Schreibweise (01 bis 12), `DD` den Tag in 2-stelliger Schreibweise (01–31), `HH` die Stunde in 2-stelliger Schreibweise (00–23), `MM` die Minute in 2-stelliger Schreibweise (00–59) und `SS` die Sekunde in 2-stelliger Schreibweise (00–59) angibt. `HH:MM:SS` ist optional. Datum und Uhrzeit werden durch eine Leerstelle getrennt.
>
> Zum Beispiel: `< 20040607 07:00:00` oder `< "20040607 07:00:00"` gibt alle Daten vor 7 Uhr am 7. Juni 2004 zurück. *Stellen Sie sicher, dass nach dem <-Operator ein Leerzeichen gesetzt ist.*

>, >= (Kleiner als oder kleiner als oder gleich)

Führt einen Zeichenfolgenvergleich aus, um alle Daten zurückzugeben, deren Wert mehr als der eingegebene Wert ist.

Zum Beispiel: `> G*` gibt alle Anwendungen aus, die mit einem Buchstaben größer als `G` beginnen.

Zum Beispiel: `> 3` gibt die Werte `3`, `3abc` und `30.129.101.76` zurück.

Agent-Version

Gibt alle Rechner mit einer angegebenen **Agent-Version** *(siehe 81)* zurück. Beispielsweise ist Agent-Version 6.2.1.1 als `6020101` angegeben.

Agentstatus

Agent > Rechnerstatus > Agent-Status

- *Agent-Status-Meldungen können über Monitoring > Benachrichtigungen > Agent-Status (siehe 286) definiert werden.*

Die Seite **Agent-Status** stellt eine Übersicht über eine Vielzahl von Agent-Daten bereit. Sie können alle Datenspalten selbst auswählen, um die Ansicht vollständig anzupassen. Spalten- und Filterauswahl gelten individuell für jeden VSA-Benutzer. Seitenzeilen können sortiert werden, indem Sie auf die Links der Spaltenüberschriften klicken.

- Über die Seite Audit > **Systeminformation** *(siehe 154)* können benutzerdefinierten Datenspalten hinzugefüt werden. Nachdem sie hinzugefügt wurden, können Sie sie auf dieser Seite und im Bericht **Gesamttabelle** anzeigen.
- Verwenden Sie die Option **Rechner zeigen, die in den letzten N Perioden nicht online / niemals online waren** in **Ansichtdefinitionen** *(siehe 27)*, um die Anzeige von Rechner-IDs auf jeder Agent-Seite zu filtern.

Spalten auswählen...

Geben Sie die Datenspalten an und die Reihenfolge, in der sie angezeigt werden sollen.

Filter...

Klicken Sie auf **Filter...** , um eine **Filtergesamttabelle anzuzeigen.** Geben Sie Zeichenfolgen ein, um die Anzeige der Zeilen im Seitenbereich zu filtern. Wenn Sie beispielsweise nach der Rechner-ID suchen möchten, bei der "jsmith" angemeldet ist, geben Sie `jsmith` in das Bearbeitungsfeld neben **Aktueller Benutzer** ein. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.

Filter zurücksetzen

Dies wird nur angezeigt, wenn ein erweiterter Filter eingestellt ist. Klicken Sie auf **Filter zurücksetzen**, um alle Zeichenfolgen zu löschen.

Spaltendefinitionen

Spalten werden in der standardmäßigen Reihenfolge beschrieben, in der sie auf dieser Seite angezeigt werden.

- **Rechner-D** – Rechner-ID-Bezeichnung, die im ganzen System verwendet wird
- **Aktueller Benutzer** – Anmeldename des gegebenenfalls aktuell am Rechner angemeldeten Benutzers
- **Letzter Neustartzeitpunkt** – Zeitpunkt des zuletzt bekannten Zeitpunkts des Rechnerneustarts
- **Letzter Check-in-Zeitpunkt** – Der letzte Zeitpunkt, an dem ein Rechner beim Kaseya Server eingecheckt war.
- **Gruppen-ID** – Gruppen-ID-Teil der Rechner-ID
- **Erster Anmeldezeitpunkt** – Der Zeitpunkt, zu dem ein Rechner sich zum ersten Mal am Kaseya Server angemeldet hat.
- **Zeitzone** – Vom Rechner verwendete Zeitzone
- **Computername** – Dem Rechner zugewiesener Computername.
- **Domäne/Arbeitsgruppe** – Arbeitsgruppe oder Domäne, zu der der Rechner gehört.
- **Arbeitsverzeichnis** – Das Verzeichnis auf dem verwalteten Rechner, das der Agent nutzt, um temporäre Dateien zu speichern.

- **DNS-Rechnername** – Vollständig qualifizierter DNS-Rechnername für den Rechner, der den Computernamen und den Domänennamen umfasst. Zum Beispiel: `jsmithxp.acme.com`. Der Rechnername wird nur angezeigt, wenn der Rechner Mitglied einer Arbeitsgruppe ist.
- **Agent-GUID** – Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
- **Betriebssystem** – Typ des Betriebssystems, das auf dem Rechner ausgeführt wird
- **BS-Version** – Versionsreihe des Betriebssystems.
- **IP-Adresse** – Dem Rechner zugewiesene IP-Adresse im Format Version 4.
- **Subnetz-Maske** – Dem Rechner zugewiesenes Netzwerksubnetz.
- **Standard-Gateway** – Dem Rechner zugewiesener Standard-Gateway.
- **Connection-Gateway** – Die vom Kaseya Server erkannte IP-Adresse, wenn dieser Rechner sich anmeldet. Befindet sich der Rechner hinter einem DHCP-Server, ist dies die öffentliche IP-Adresse des Subnetzes.
- **Land** – Mit dem Connection-Gateway verknüpftes Land.
- **IPv6 Adresse** – Dem Rechner zugewiesene IP-Adresse im Format Version 6.
- **MAC-Adresse** – MAC-Adresse der LAN-Karte, die zur Kommunikation mit dem Kaseya Server verwendet wird.
- **DNS-Server 1, 2** – IP-Adresse des dem Rechner zugewiesenen DNS-Servers.
- **DHCP-Server** – IP-Adresse des von diesem Rechner verwendeten DHCP-Servers.
- **Primärer/Sekundärer WINS** – WINS-Einstellungen.
- **CPU-Typ** – Prozessorversion und -modell.
- **CPU-Geschwindigkeit** – Taktgeschwindigkeit des Prozessors.
- **Prozessorzahl** – Anzahl der Prozessoren.
- **RAM-Größe** – MByte an RAM auf dem Rechner.
- **Agent-Version** – Versionsnummer des auf dem Rechner geladenen Kaseya-Agents.
- **Letzter angemeldeter Benutzer** – Anmeldename des zuletzt am Rechner angemeldeten Benutzers.
- **Portalzugriffsanmeldung** – Der einem Rechnerbenutzer zugewiesene Anmeldename zur Anmeldung am Kaseya Server.
- **Portalzugriff-Fernsteuerung** – Dies ist aktiviert, wenn sich dieser Rechnerbenutzer anmelden und die Fernsteuerung *zu seinem eigenen Rechner von einem anderen Rechner aus* aktivieren kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Portalzugriff-Ticketing** – Dies ist aktiviert, wenn sich dieser Rechnerbenutzer anmelden und Tickets eingeben kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Portalzugriff-Chat** – Dies ist aktiviert, wenn dieser Rechnerbenutzer Chat-Sitzungen mit einem VSA-Benutzer *einleiten* kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Primärer/Sekundärer KServer** – Vom Rechner verwendete IP-Adresse und Name zur Kommunikation mit dem Kaseya Server.
- **Intervall für Schnellanmeldung** – Zeiteinstellung für **Schnellanmeldung** *(siehe 616)* in Sekunden.
- **Kontaktname** – Unter **Profil bearbeiten** *(siehe 73)* eingegebener Rechnerbenutzername.
- **Kontakt E-Mail** – E-Mail-Adresse wie in "Profil bearbeiten" eingegeben.
- **Kontakt-Telefon** – In "Profil bearbeiten" eingegebene Telefonnummer.
- **Kontakthinweise** – In "Profil bearbeiten" eingegebene Anmerkungen.
- **Hersteller** – Systemhersteller.
- **Produktname** – Produktname des Systems.
- **Systemversion** – Versionsnummer des Produkts.
- **System-Seriennummer** – Seriennummer des Systems.
- **Gehäuse-Seriennummer** – Seriennummer auf dem Gehäuse.
- **Gehäuse-Bestandsetikett** – Bestandsetikett auf dem Gehäuse.
- **Externe Busgeschwindigkeit** – Busgeschwindigkeit des Motherboards.
- **Max. Speichergröße** – Maximale Speichergröße des Motherboards.

- **Max. Speichersteckplätze** – Gesamtzahl der verfügbaren Speichermodulsteckplätze.
- **Gehäusehersteller** – Hersteller des Gehäuses.
- **Gehäusetyp** – Typ des Gehäuses.
- **Gehäuseversion** – Versionsnummer des Gehäuses.
- **Motherboard-Hersteller** – Hersteller des Motherboards.
- **Motherboard-Produkt-ID** – Produkt-ID des Motherboards
- **Motherboard-Version** – Versionsnummer des Motherboards.
- **Motherboard-Seriennummer** – Seriennummer des Motherboards.
- **Prozessorfamilie** – Installierter Prozessortyp.
- **Prozessorhersteller** – Hersteller des Prozessors.
- **Prozessorversion** – Versions-ID des Prozessors.
- **Max. CPU-Geschwindigkeit** – Maximal unterstützte Prozessorgeschwindigkeit.
- **Aktuelle CPU-Geschwindigkeit** – Aktuelle Geschwindigkeit des Prozessors
- **vPro-Hostname** – Von der vPro-Konfiguration eingestellter Name des vPro-fähigen Rechners.
- **vPro-Computername** – Vom Betriebssystem eingestellter Name des vPro-fähigen Rechners.
- **vPro-Modell** – Modell des vPro-fähigen Rechners.
- **vPro-Hersteller** – Hersteller des vPro-fähigen Rechners.
- **vPro-Version** – Version des vPro-fähigen Rechners.
- **vPro-Seriennummer** – Seriennummer des vPro-fähigen Rechners.
- **vPro-Bestandsnummer** – Identifikator zur Bestandsverwaltung, der dem vPro-fähigen Rechner zugewiesen wurde.
- **Hersteller des vPro-Motherboards** – Hersteller des Motherboards auf dem vPro-fähigen Rechner.
- **Produktname des vPro-Motherboards** – Produktname des Motherboards auf dem vPro-fähigen Rechner.
- **Version der vPro-Motherboards** – Versionsnummer des Motherboards auf dem vPro-fähigen Rechner.
- **Seriennummer der vPro-Motherboards** – Seriennummer des Motherboards auf dem vPro-fähigen Rechner.
- **Bestandsetikett der vPro-Motherboards** – Identifikator zur Bestandsverwaltung, der dem Motherboards des vPro-fähigen Rechners zugewiesen wurde.
- **Anbieter des vPro-Bios** – Anbieter des BIOS des vPro-fähigen Rechners.
- **Version des vPro-Bios** – Version des BIOS des vPro-fähigen Rechners.
- **Freigabedatum des vPro-Bios** – BIOS-Freigabedatum des vPro-fähigen Rechners

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Agentprotokolle

Agent > Rechnerstatus > Agent-Protokolle

Die Seite **Agent-Protokolle** zeigt Protokolldaten zu verwalteten Rechnern an. Für jede Art des Protokolls gibt es entsprechende **Protokollberichte** *(siehe 164)*.

> **Hinweis:** Das System begrenzt die Anzahl der Protokolleinträge pro Protokolltyp pro Rechner automatisch auf 1.000. Sobald das Limit erreicht wird, werden die darüber liegenden Protokolleinträge archiviert (falls die Archivierung aktiviert ist) und aus dem System gelöscht. Die Archivoption wird in **Protokollverlauf** *(siehe 36)* eingestellt.

Rechner-ID

Klicken Sie auf den Hyperlink einer Rechner-ID, um alle Protokolle dieser Rechner-ID zu listen.

Protokoll auswählen

Wählen Sie ein Protokoll aus der Dropdown-Liste **Protokoll auswählen**. Es gibt folgende Protokollarten:

- **Alarmprotokoll** – Listet alle ausgelösten Alarme für den ausgewählten Rechner auf.
- **Monitor-Aktionsprotokoll** – Das Protokoll der **Meldungsbedingungen** *(siehe 621)* sowie die entsprechenden Aktionen, die als Reaktion darauf ergriffen wurden.

  > **Hinweis:** Ein Zählerwert von -008 in den Kontrollprotokollen gibt an, dass der Monitorset keine Daten zurückgibt. Überprüfen Sie, dass der `Performance Logs & Alerts`-Dienst in Windows ausgeführt wird. Dies ist eine Voraussetzung für die Überwachung der Leistungszähler.

- **Agent-Protokoll** – Zeigt ein Protokoll der Agent-, System- und Fehlermeldungen an.
- **Konfigurationsänderungen** – Zeigt Änderungen an den VSA-Einstellungen für den ausgewählten Rechner an.
- **Netzwerkstatistiken** – Zeigt ein Protokoll vpn Daten senden/empfangen für Netzwerkanwendungen an.

  > **Hinweis:** Für dieses Protokoll muss der Treiber Audit > **Netzwerkzugriff** *(siehe 84)* aktiviert sein. Dieser Treiber fügt sich in den TCP/IP-Stapel ein, um den auf dem TCP/IP-Protokoll basierenden Datenverkehr nach Anwendung zu messen. Er ist standardmäßig *deaktiviert*.

- **Ereignisprotokolle** – Zeigt die von Windows gesammelten Ereignisprotokolldaten an. Dies ist nicht für Win9x verfügbar. In der Dropdown-Liste des Ereignisprotokolls werden nur Ereignisprotokolle angezeigt, die auf den ausgewählten Rechner zutreffen. Ein gibt einen als Warnung klassifizierten Protokolleintrag an. Ein gibt einen als Fehler klassifizierten Protokolleintrag an. Ein gibt einen als Information klassifizierten Protokolleintrag an.

  Ein Monitor-Assistent--Symbol wird neben dem Ereignisprotokolleintrag im VSA und in **Live Connect** angezeigt. Durch Klicken auf das Monitor-Assistent-Symbol eines Protokolleintrags wird ein Assistent angezeigt. Der Assistent ermöglicht Ihnen auf Basis dieses Protokolleintrags ein neues Kriterium für den Ereignissatz zu erstellen. Das neue Ereignissatz-Kriterium kann zu jedem neuen oder bestehenden Ereignissatz hinzugefügt werden. Der neue oder geänderte Ereignissatz wird sofort auf den Rechner angewendet, der die Quelle dieses Protokolleintrags war. Wird ein bestehender Ereignissatz geändert, so sind alle Rechner davon betroffen, denen dieser Ereignissatz zugeordnet ist. Das Monitor-Assistent-Symbol wird angezeigt in:

  - Agent>Agent-Protokolle
  - Live Connect > Ereignisanzeige

➢ Live Connect > Agent-Daten > Ereignisprotokoll

Siehe Monitor > **Ereignisprotokoll-Meldungen** *(siehe 316)* – hier ist jedes im Assistenten angezeigte Feld beschrieben.

- **Agent-Verfahrensprotokoll** – Protokoll der erfolgreichen/fehlgeschlagenen Agent-Verfahren.
- **Fernsteuerungsprotokoll** – Zeigt ein Protokoll der erfolgreichen/fehlgeschlagenen Fernsteuerungssitzungen an.
- **Protokoll-Monitoring** – Zeigt Einträge des **Protokoll-Monitoring** *(siehe 626)* an.

Ereignisse pro Seite

Wählen Sie die Anzahl der Zeilen aus, die pro Seite angezeigt werden sollen.

Startdatum/ Enddatum/Aktualisieren

Wählen Sie einen Datumsbereich zum Filtern der Protokolldaten aus und klicken Sie dann auf die Schaltfläche **Aktualisieren**.

Filter...

Gilt nur für `Event Logs`. Klicken Sie auf **Filter...**, um die Menge der angezeigten Daten einzuschränken. Für jede angezeigte Ereigniskategorie und Datenspalte kann ein anderer erweiterter Filter angegeben werden.

Ereignisprotokollfilter anwenden

Gilt nur für `Event Logs`. Der Ereignisprotokollfilter enthält Optionen, die über die Schaltfläche **Filter...** definiert werden. Wenn **Ereignisprotokollfilter anwenden** aktiviert ist, wird die Filterung angewendet.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Protokollhistorie

Agent > Rechnerstatus > Protokollverlauf

Auf der Seite **Protokollverlauf** wird die Anzahl der Tage festgelegt, für die Protokolldaten auf einer Pro-Protokoll-Basis für jede Rechner-ID in der Datenbank gespeichert werden. Protokolldaten werden über **Agent-Protokolle** *(siehe 35)* angezeigt oder mit Info Center > Reporting > Protokolle ausgedruckt. Außerdem wird auf dieser Seite festgelegt, ob Agent-Protokolldaten später in Textdateien in einem Netzwerkverzeichnis archiviert werden. Das Verzeichnis wird mit System > Serververwaltung > **Konfigurieren** *(siehe 429)* bezeichnet. Mithilfe dieser Seite vorgenommene Änderungen werden beim nächsten Agent-Check-in wirksam und bis dahin als roter Text angezeigt.

- **Protokolleinstellungen** können auch mithilfe der Registerkarte **Agent-Einstellungen** von **Live-Connect** *(siehe 393)* > Agentdaten oder der Seite **Rechnerübersicht** *(siehe 151)* gepflegt werden.
- System > Systemeinstellungen > **Check-in-Richtlinie** *(siehe 405)* kann die Anzahl der Tage einschränken, für die Benutzer die Protokolleinträge behalten können, um eine unnötige Last auf den Servern zu vermeiden, auf denen der Kaseya Server-Dienst ausgeführt wird.
- Diese Einstellungen werden standardmäßig aus dem Agent-Installationspaket übernommen. Agent-Installationspakete werden über Agent > **Agent einrichten** *(siehe 40)* erstellt.

Größenanforderungen der Datenbank schätzen

Je mehr Daten Sie protokollieren, desto größer wird die Datenbank. Die Größenanforderungen der Datenbank können unterschiedlich sein. Es kommt auf die Anzahl der bereitgestellten Agents und die aktivierte Protokollierungsstufe an. Um die Größenanforderungen der Datenbank für Protokolldaten zu

schätzen, erstellen Sie einen Auszug der `nteventlog`-Tabelle der Datenbank. Legen Sie fest, wie viele Daten pro Tag protokolliert werden und schätzen Sie dann anhand dieses Werts den zusätzlichen Speicherplatz ein, der für ein längeres Speichern der Protokolle erforderlich ist.

Anzahl Tage festlegen, die Protokolleinträge aufbewahrt werden sollen. Markieren, um Einträge in Datei zu archivieren

Legen Sie die Anzahl der Tage fest, für die Protokolleinträge für jede Art von Protokoll aufbewahrt werden sollen. Aktivieren Sie das Kontrollkästchen für jedes Protokoll, um Protokolldateien nach ihrem Enddatum zu archivieren.

- **Konfigurationsänderungen** – Protokoll der von jedem Benutzer vorgenommenen Konfigurationsänderungen.
- **Netzwerkstatistiken** – Protokoll der ein- und ausgehenden Paketzahlinformationen und der Anwendung oder des Prozesses, die/der solche Pakete überträgt und/oder empfängt. Die Informationen können im Detail über Agent > **Agent-Protokolle** *(siehe 35)* > Netzwerk-Statistik angezeigt werden.
- **Agent-Verfahrensprotokoll** – Protokoll der erfolgreichen/fehlgeschlagenen Agent-Verfahren.
- **Fernsteuerungsprotokoll** – Protokoll der Fernsteuerungsereignisse.
- **Alarmprotokoll** – Protokoll aller ausgegebenen Alarme.
- **Monitoring-Aktion** – Protokoll der aufgetretenen Meldungsbedingungen sowie die entsprechenden Aktionen, die als Reaktion darauf ergriffen wurden.
- **SYS-Protokoll** – Das Protokoll "Protokollüberwachung".
- **Agent-Betriebszeitprotokoll** – Protokolliert den Betriebsverlauf von Agents. Anzahl der Tage muss auf 1 oder höher gesetzt sein, um eine genaue Zeiterfassung des letzten Neustarts zu erhalten. Siehe **Erfassen der letzten Neustartzeiten für den Agent** *(https://helpdesk.kaseya.com/entries/35994418)* und **Schaltfläche "Jetzt neu starten" bleibt und/oder Endbenutzer meldet fortlaufenden Reboot-Nag nach Neustart https://helpdesk.kaseya.com/entries/33901207**.

> **Hinweis:** Alle oben aufgelisteten Agent-Protokollarchive werden in dem vom Feld System > Serververwaltung > **Konfigurieren** *(siehe 429)* > **Pfad des Protokolldateiarchivs** angegebenen Verzeichnis gespeichert.

Festlegen, wie viele Tage die Monitor-Protokolle für alle Rechner aufbewahrt werden sollen

Die folgenden Monitoring-Protokolleinstellungen werden systemweit angewendet.

- **Ereignisprotokoll** – Protokoll aller Ereignisse. Die erfassten Ereignisse werden detaillierter über Agent > **Ereignisprotokolleinstellungen** *(siehe 38)* angegeben.
- **Monitoring-Protokoll** – Protokoll der von Monitor-Sets erfassten Daten
- **SNMP-Protokoll** – Protokoll aller von SNMP-Sets erfassten Daten.
- **Agent-Protokoll** – Protokoll der Agent-, System- und Fehlermeldungen

> **Hinweis:** Die Protokollarchive der Monitoring-Daten auf der Seite "Agent > **Protokollhistorie** *(siehe 36)*" werden im Verzeichnis `<KaseyaRoot>\UserProfiles\@dbBackup` gespeichert. Damit soll die Leistung von Systemen verbessert werden, bei denen sich die Datenbank auf einem anderen Server befindet. Alle anderen Agent-Protokollarchive werden in dem im Feld "System > **Konfigurieren** *(siehe 429)* > **Pfad des Protokolldateiarchivs**" angegebenen Verzeichnis gespeichert.

Alle Tage festlegen

Klicken Sie auf **Alle Tage festlegen**, um alle Tag-Felder auf denselben Wert einzustellen.

Alle Archive auswählen/Alle Archive abwählen

Klicken Sie auf den Link **Alle Archive auswählen**, um alle Archiv-Kontrollkästchen auf der Seite zu

markieren. Klicken Sie auf den Link **Alle Archive abwählen**, um alle Archiv-Kontrollkästchen auf der Seite zu deaktivieren.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um ausgewählte Rechner-IDs mit AgentProtokolleinstellungen zu aktualisieren.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Ereignisprotokolleinstellungen

Agent > Rechnerstatus > Ereignisprotokolleinstellungen

Die Seite **Ereignisprotokolleinstellungen** gibt die Kombination von **Ereignisprotokoll** *(siehe 618)*-Typen und -Kategorien an, die vom VSA erfasst werden.

> **Hinweis:** Meldungen können mit Monitoring > **Ereignisprotokollmeldungen** *(siehe 316)* separat für Ereignisse angegeben werden. **Ereignisprotokollmeldungen werden auch noch erstellt, wenn Ereignisprotokolle nicht vom VSA erfasst werden.**

So legen Sie **Ereignisprotokolleinstellungen** fest:

1. Klicken Sie im Listenfeld **Ereignisprotokolltypen** auf einen Ereignisprotokolltyp. Halten Sie die [Strg]-Taste gedrückt, um mehrere Ereignisprotokolltypen auszuwählen.
2. Klicken Sie auf **Hinzufügen>**, um Ereignisprotokolltypen zum Listenfeld **Zugewiesene Ereignistypen** hinzuzufügen. Klicken Sie auf **<< Entfernen** oder **<< Alle entfernen**, um Ereignisprotokolltypen aus dem Listenfeld **Zugewiesene Ereignistypen** zu entfernen.
3. Markieren Sie eine oder mehrere Ereigniskategorien: **Fehler, Warnung, Informationen, Audit erfolgreich, Audit fehlgeschlagen, Kritisch, Verbose.**
4. Wählen Sie eine oder mehrere Rechner-IDs aus.
5. Klicken Sie auf **Aktualisieren** oder **Ersetzen**, um diese Einstellungen auf ausgewählte Rechner-IDs anzuwenden.

Globale Ereignisprotokolllisten

Jeder Agent verarbeitet zwar alle Ereignisse, die auf einer "Blacklist" aufgeführten Ereignisse werden jedoch *nicht* auf den VSA-Server hochgeladen. Es gibt zwei "Blacklists". Eine wird periodisch von Kaseya aktualisiert und trägt die Bezeichnung `EvLogBlkList.xml.`. Die zweite mit dem Namen `EvLogBlkListEx.xml` kann vom Dienstanbieter verwaltet werden und wird nicht von Kaseya aktualisiert. Beide befinden sich im Verzeichnis `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles`. Die Alarmermittlung und -verarbeitung werden fortgesetzt, ungeachtet dessen, ob sich die Einträge in der Erfassungs-Blacklist befinden oder nicht.

Fluterkennung

Wenn 1000 Ereignisse (ohne Zählung der **Blacklist-Ereignisse** *(siehe 619)*) von einem Agent *innerhalb einer Stunde* auf den Kaseya Server hochgeladen werden, wird die weitere Erfassung von Ereignissen dieses Protokolltyps für den Rest der Stunde angehalten. Ein neues Ereignis wird in das Ereignisprotokoll eingefügt, um die Aussetzung der Erfassung zu verzeichnen. An Ende der Stunde wird die Erfassung automatisch wieder aufgenommen. Dies verhindert, dass der Kaseya Server von kurzfristigen Schwerlasten überschwemmt wird. Die Alarmermittlung und -verarbeitung wird ungeachtet einer ausgesetzten Erfassung fortgesetzt.

Aktualisieren

Fügt die im Listenfeld **Zugewiesene Ereignistypen** aufgeführten Ereignisprotokolltypen zum Satz der Ereignisprotokolltypen hinzu, die bereits ausgewählten Rechner-IDs zugewiesen wurden.

Ersetzen

Ersetzt alle den ausgewählten Rechner-IDs zugewiesenen Ereignisprotokolltypen durch die Ereignisprotokolltypen, die in der Liste **Zugewiesene Ereignistypen** aufgeführt werden.

Alle löschen

Löscht alle Ereignisprotokolltypen, die ausgewählten Rechner-IDs zugewiesen wurden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol ✗, um diesen Datensatz zu löschen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol neben einer Rechner-ID, um automatisch Kopfzeilenparameter einzustellen, die mit denjenigen der ausgewählten Rechner-ID übereinstimmen.

Zugewiesene Kategorien

Dies sind die Ereigniskategorien, die vom VSA für diese Rechner-ID und das Ereignisprotokoll gespeichert werden:

- **F**ehler
- **W**arnung
- **I**nformationen
- **A**udit erfolgreich
- **A**udit fehlgeschlagen
- **K**ritisch – betrifft nur Vista, Windows 7 und Windows Server 2008
- **V**erbose – betrifft nur Vista, Windows 7 und Windows Server 2008

Agents verteilen

Agent > Agents installieren > Agents bereitstellen

Auf der Seite **Agent bereitstellen** wird ein Agent-Installationspaket erstellt und auf *mehreren* Rechnern bereitgestellt.

Agent-Installationspakete

Agents werden auf verwalteten Rechnern über ein **Agent-Installationspaket** installiert. Ein Agent-Installationspaket enthält alle Einstellungen, mit denen ein Agent auf einem Zielrechner funktionieren soll.

Die Seite Agent > **Agent bereitstellen** zeigt die in Ihrem VSA verfügbaren Agent-Installationspakete an. Ein `Default Install`-Paket wird mit dem VSA bereitgestellt. Es werden möglicherweise andere Agent-Installationspakete angezeigt, die bereits erstellt und auf dieser Seite aufgelistet wurden.

Ein Agent-Installationspaket wird über den Assistenten **Automatische Kontenerstellung konfigurieren** erstellt. Der Assistent kopiert Agent-Einstellungen von einer *vorhandenen* Rechner-ID oder Rechner-ID-Vorlage und erstellt ein Installationspaket mit der Bezeichnung `KcsSetup.`. Alle Einstellungen und ausstehenden Agent-Verfahren für die Rechner-ID, von der Sie kopieren – abgesehen von Rechner-ID, Gruppen-ID und Organisations-ID – werden auf jede neue Rechner-ID angewendet, die mit dem Paket erstellt wird.

> **Hinweis:** Weitere Hinweise finden Sie in der PDF-Schnellstartanleitung **Agent-Konfiguration und Verteilung** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_agentdeployment70.pdf#view=Fit&navpanes=0).*

Weitere Themen

- **Agent-Installationspaket erstellen** *(siehe 41)*
- **Manuelle Installation des Agents** *(siehe 42)*
- **Automatisieren der Agent-Installation** *(siehe 43)*
- **Agent-Installationspakete pflegen** *(siehe 44)*
- **Agent-Einstellungen konfigurieren** *(siehe 45)*
- **Befehlszeilenschalter für Agent-Installation** *(siehe 48)*
- **Probleme und Fehler bei der Installation** *(siehe 49)*

- **Mehrere Agents installieren** *(siehe 50)*
- **Installation von Linux Agents** *(siehe 52)*
- **Unterstützte Linux Funktionen** *(siehe 53)*
- **Unterstützte Apple-Funktionen** *(siehe 54)*

Aktionen

- **Hier klicken, um den Standard-Agent herunterzuladen** – Klicken Sie auf diesen Link, um das Standardpaket des aktuellen VSA-Benutzers direkt von dieser Seite herunterzuladen.
- **Benutzer können Agents herunterladen von** – Fügen Sie diesen Hyperlink in eine E-Mail-Nachricht ein. Die *eindeutige ID-Nummer* stellt sicher, dass beim Klicken auf den Link in der E-Mail-Nachricht das Standard-Installationspaket ausgewählt und heruntergeladen wird. Stellen Sie ein anderes Installationspaket als Standard ein, um den Link für dieses Installationspaket anzuzeigen.
- **Pakete aller Administratoren verwalten** – Aktivieren Sie dieses Kontrollkästchen, um alle von allen VSA-Benutzern erstellten Pakete anzuzeigen. Nachdem ein verborgenes Paket angezeigt wurde, können Sie es verwenden oder öffentlich machen. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

Tabellenspalten

- **Standard einrichten** – Geben Sie Ihr eigenes Standard-Installationspaket an, indem Sie das Optionsfeld links neben dem Paketnamen in der Spalte **Standard einrichten** auswählen.
- **Löschen-Symbol** – Klicken Sie auf das Löschen-Symbol ✕, um ein Paket aus dem Seitenbereich zu entfernen. Wenn das Paket von Ihnen erstellt wurde, wird es ebenfalls aus dem System gelöscht und aus allen Listen der VSA-Benutzer entfernt.
- **Bearbeitungssymbol** – Klicken Sie auf das Bearbeitungssymbol neben einem Paket, um mithilfe des Assistenten **Automatische Kontenerstellung konfigurieren** die Parameter für dieses Paket zu ändern.
- **Paketname** – Listet den Namen des Pakets auf.
- **Öffentliches Paket** – Die Zeilen in öffentlichen Paketen werden mit einem braunen Hintergrund angezeigt. Die Zeilen in privaten Paketen werden mit einem grauen Hintergrund angezeigt.
- **Gemeinsam nutzen** – Klicken Sie auf **Gemeinsam nutzen**, damit Sie ein privates Paket mit anderen Benutzern und Benutzerrollen **gemeinsam nutzen** *(siehe 421)* oder das Paket öffentlich machen können.
- **Liste in dl.asp** – Klicken Sie auf den Link **dl.asp** im Spaltenkopf, um die Webseite anzuzeigen, die Rechnerbenutzer beim Installieren eines Agents auf ihrem Rechner sehen. Aktivieren Sie ein Kontrollkästchen in dieser Spalte, um ihr Paket in die Liste der verfügbaren Download-Pakete auf der Seite **dl.asp** aufzunehmen.
- **Beschreibung** – Zeigt die Beschreibung des Pakets an.

Agent-Installationspaket erstellen

Klicken Sie auf der Seite Agent > **Agents bereitstellen** *(siehe 40)* auf **Paket erstellen**, um den Assistenten **Automatische Kontenerstellung konfigurieren** zu starten. Der Assistent ist ein Verfahren mit 7 Schritten.

1. Definieren Sie Regeln für die Benennung der Rechner-ID.
   - Fordern Sie den Benutzer auf, eine Rechner-ID einzugeben.
   - Verwenden Sie den Rechnernamen als Rechner-ID.
   - Stellen Sie den Benutzernamen des gegenwärtig angemeldeten Benutzers als Rechner-ID ein.
   - Geben Sie eine feste Rechner-ID für dieses Installationspaket an.
2. Definieren Sie Regeln für die Benennung der Gruppen-ID.
   - **Bestehende Gruppe** – Wählen Sie eine vorhandene Gruppen-ID aus einer Dropdown-Liste aus.

- **Domänen-Name** – Verwenden Sie den Domänen-Namen des Benutzers.
- **Neue Gruppe** – Geben Sie eine neue Gruppen-ID an. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- **Benutzer auffordern** – Der Benutzer wird zur Eingabe einer Gruppen-ID aufgefordert. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

3. Geben Sie **Befehlszeilenschalter** *(siehe 48)* für das Agent-Installationspaket an, einschließlich der Möglichkeit, die Installation **automatisch ohne Taskleisten oder Dialogfelder** *(siehe 616)* auszuführen.
4. Geben Sie die Rechner-ID an, von der Einstellungen und anstehende Agent-Verfahren kopiert werden sollen. Sämtliche Einstellungen und anstehenden Agent-Verfahren (außer der Rechner-ID, Gruppen-ID und Organisations-ID) werden auf jede neue, mit dem Paket erstellte Rechner-ID angewendet.

> **Hinweis:** Die Anweisung `Copy settings from unknown.root.unnamed if nothing selected` basiert auf der Rechner-ID oder -Vorlage, die vom Standard-Installationspaket ausgewählt wurde.

5. Wählen Sie das Betriebssystem aus, für das Sie das Installationspaket erstellen: `Automatically choose OS of downloading computer:` `Windows`, `Macintosh` oder `Linux.`
6. Binden Sie optional die Anmeldedaten eines Benutzers an das Installationspaket. Füllen Sie das Formular **Administratoranmeldedaten** aus, um die Benutzerrechte sicher an das Installationsformular zu binden.
   - Benutzer ohne Administratorrechte können das Installationspaket erfolgreich installieren, ohne Administrator-Anmeldedaten eingeben zu müssen.
   - Wenn die Administrator-Anmeldedaten leer gelassen werden und der Benutzer keine Administratorrechte zum Installieren von Software hat, wird er während der Installation vom Installationspaket zur Eingabe von Administrator-Anmeldedaten aufgefordert. **Falls das Paket automatisch installiert wird, schlägt `KcsSetup` fehl, ohne dass die Gründe hierfür in irgendwelchen Dialogmeldungen angezeigt werden.**

> **Administratoranmeldedaten** – Gegebenenfalls kann ein Agent-Installationspaket erstellt werden, das Anmeldedaten eines Administrators für den Zugriff auf ein Kundennetzwerk enthält. Anmeldedaten sind nur erforderlich, wenn Benutzer Pakete auf Rechnern installieren und keinen Administratorzugriff auf ihr Netzwerk haben. Die Anmeldedaten des Administrators sind verschlüsselt, niemals als Klartext verfügbar und an das Installationspaket gebunden.

7. Benennen Sie das Installationspaket, damit später leicht darauf verwiesen werden kann. Dieser Name wird auf der Seite **Agents bereitstellen** und der Download-Seite `dl.asp` angezeigt.

Manuelle Installation des Agents

Installationspakete von der Seite "Agent bereitstellen" manuell herunterladen

Auf der Seite **Agent bereitstellen** werden drei Arten von Links zum Herunterladen von Agent-Installationspaketen zur Verfügung gestellt:

- **Klicken Sie auf den Link "Standard-Agent herunterladen"** – Jeder Benutzer besitzt sein eigenes Standard-Agent-Installationspaket. Klicken Sie auf diesen Link, um Ihren eigenen Benutzer-Standard-Agent herunterzuladen.
- **Klicken Sie auf den Link "Paket"** – Die vollständige Liste von verfügbaren Agent-Installationspaketen wird auf der Seite **Agents bereitstellen** angezeigt. Klicken sie auf einen dieser Links, um das Agent-Installationspaket herunterzuladen.
- **Klicken Sie auf den Link "dl.asp"** – Auf der `dl.asp`-Webseite werden alle öffentlich verfügbaren Agent-Installationspakete aufgelistet. Klicken Sie auf ein beliebiges Paket auf der "dl.asp"-Webseite, um es herunterzuladen.

Mit jeder dieser Methoden wird die gleiche `KcsSetup`-Datei zum Installieren des Agents heruntergeladen.

Installieren eines Agents mithilfe der dl.asp Page

Die folgende ist die schnellste Methode für die manuelle Installation eines Agents.

1. Melden Sie sich bei dem Rechner an, auf dem der Agent installiert werden soll.
2. Geben Sie die folgende URL in den Browser des Rechners ein:
   `http://<YourVSAaddress>/dl.asp`
3. Klicken Sie auf das Paket `Default Install`, um die Installation des Agent auf dem Rechner zu starten.
   - Falls noch andere Installationspakete aufgeführt sind, wählen Sie Ihr bevorzugtes Paket aus.
   - Im Verlauf der Installation müssen Sie möglicherweise eine Bestätigung eingeben, damit der Vorgang abgeschlossen werden kann.
4. Melden Sie sich bei VSA an:
   `http://<YourVSAaddress>`
5. Wählen Sie im VSA die Seite Agent > **Agent-Status** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#250.htm)*.

Auf der Seite sollte jetzt ein neues Rechnerkonto für den soeben erstellten Agent angezeigt werden.

Ausführen des Agent-Installationspakets auf dem Endpunktrechner

Benutzer können das `KcsSetup`-Installationsprogramm auf dem Endpunktrechner auf folgende Arten ausführen:

- *Fenster*
  - Doppelklicken Sie auf `KcsSetup`, um es zu starten.
  - Öffnen Sie ein **Befehlszeilenfenster** und geben Sie `KcsSetup` gefolgt von jeden gewünschten **Befehlszeilenschaltern** *(siehe 48)* ein.
  - Wählen Sie **Ausführen...** im **Windows-Startmenü** und geben Sie `KcsSetup` gefolgt von jeden gewünschten Befehlszeilenschaltern ein.
- *Apple und Linux*
  - Doppelklicken Sie auf `KcsSetup`, um es zu starten.
  - Der vollständige Dateiname für ein Macintosh-Agent-Installationspaket lautet `KcsSetup.app`. `KcsSetup.app` wird als ein `KcsSetup.zip` heruntergeladen, was `KcsSetup.app` innerhalb eines Ordners mit dem Titel `Agent` enthält. Klicken Sie auf die `KcsSetup.zip`-Datei, um sie zu erweitern, klicken Sie dann auf den Ordner `Agent` und anschließend auf die Datei `KcsSetup.app`, um diese auszuführen.

Hinweis: Bei Apple können **Befehlszeilenschalter** *(siehe 48)* nur für die Erstellung des Agent-Installationspaketes verwenden werden.

Hinweis: Bei Linux erhalten Sie weitere Informationen unter **Installation von Linux Agents** *(siehe 52)*.

Neuinstallieren von Agents

Auf der Seite **Erstellen** *(siehe 55)* können Sie einen Agent für ein vorhandenes Rechner-ID-Konto neu installieren.

Automatisieren der Agent-Installation

Mithilfe der folgenden Methoden können Sie die Installation von Agent-Installationspaketen automatisieren:

Login

- **Windows** – Richten Sie ein **NT-Anmelde**verfahren ein, um das Installationspaket jedes Mal auszuführen, wenn sich ein Benutzer am Netzwerk anmeldet. Siehe Systemveraussetzungen.
- **Apple** – Richten Sie ein **Apple OS X Login Hook-Verfahren** ein, um das Installationspaket jedes Mal auszuführen, wenn sich ein Benutzer am Netzwerk anmeldet. Siehe Kaseya KB-Artikel **HT2420** *(http://support.apple.com/kb/HT2420)*.

Verfahren

1. Erstellen Sie das Bereitstellungspaket mithilfe des Assistenten Agent > **Agents bereitstellen**.
   - Das `KcsSetup`-Installationsprogramm überspringt die Installation, wenn es feststellt, dass sich bereits ein Agent auf einem Rechner befindet, falls der Schalter `/e` im Installationspaket vorliegt.
   - Sie werden wahrscheinlich die Option der automatischen Installation wählen.
   - Falls Benutzer, die das Anmeldeverfahren ausführen, keine Benutzerrechte haben, müssen gegebenenfalls Administrator-Anmeldedaten eingebunden werden.
2. Laden Sie über die Seite `dl.asp` das entsprechende `KcsSetup`-Installationspaket herunter und kopieren Sie es in eine Netzwerkfreigabe, von der aus Benutzer Programme ausführen können.
3. Fügen Sie die Datei `KcsSetup` mit ihrem Netzwerkpfad zum Anmeldeverfahren hinzu.

E-Mail

Senden Sie `KcsSetup` per E-Mail an alle Benutzer im Netzwerk. Laden Sie das entsprechende Installationspaket von der Seite **Agents bereitstellen** herunter und hängen Sie es an eine E-Mail auf Ihrem lokalen Rechner an. Sie können den Link des Standard-Installationspakets auch kopieren und in eine E-Mail-Nachricht einfügen. Fügen Sie Anleitungen zum Starten des Pakets ein, wie im nachstehenden Aufzählungspunkt **Manuell** beschrieben.

Ermittlung nach Netzwerk oder Domain

Verwenden Sie das **Discovery**-Modul, um Rechner in **Netzwerken** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* und **Domains** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#10750.htm)* zu ermitteln. Installieren Sie dann die Agents manuell oder automatisch auf ermittelten Rechnern.

Automatische Kontenerstellung

Die *automatische Kontenerstellung muss* über System > **Check-in-Richtlinie** aktiviert werden, damit Sie automatisch ein Rechner-ID-Konto erstellen können, wenn ein Agent-Installationspaket installiert wird. Diese Option wird beim Installieren des VSA standardmäßig aktiviert.

Rechnergruppen neue Rechner-IDs nach IP-Adresse zuweisen

Sie können auch ein generisches Installationspaket erstellen, mit dem alle neuen Rechnerkonten zu der `unnamed` Gruppen-ID hinzugefügt werden. Wenn sich der Agent das erste Mal anmeldet wird ihm mit System > **Benennungsrichtlinie** die korrekte Gruppen-ID bzw. Untergruppen-ID unter Verwendung der IP-Adresse des verwalteten Rechners zugewiesen. Agent-Einstellungen können anschließend nach Richtlinie oder Vorlage konfiguriert werden. Siehe:

- **Konfigurieren von Agent-Einstellungen mit Richtlinien** *(siehe 46)*
- **Konfigurieren von Agent-Einstellungen mit Vorlagen** *(siehe 46)*

Agent-Installationspakete pflegen

Aktualisieren der Agent-Software

Ein Agent-Installationspaket lädt immer einen `KcsSetup.exe` herunter, der die neueste verfügbare Version der Agent-Software verwendet. Sobald die Datei `KcsSetup.exe` erstellt ist, bleibt ihre Version

der Agent-Software innerhalb der exe-Datei fest. Erwägen Sie, `KcsSetup.exe`-Dateien zu ersetzen, die vor einer Weile erstellt und dann für eine einfache Verteilung in Netzwerkverzeichnissen gespeichert oder zu CDs hinzugefügt wurden. Auf gleiche Weise bleibt die auf dem Rechner installierte Version der Agent-Software immer fest, bis Sie sie über die Seite **Agent aktualisieren** *(siehe 81)* aktualisieren.

Standard-Installationspaket bearbeiten

Das `Default Install`-Paket stellt die Standardwerte ein, die beim Erstellen eines neuen Pakets angezeigt werden. Normalerweise kann das `Default Install`-Paket nicht geändert werden. Die Schaltfläche **Speichern** ist deaktiviert. Um die Schaltfläche **Speichern** für das `Default Install`-Paket zu aktivieren, führen Sie Folgendes *als Benutzer mit Master-Rolle* aus:

1. Klicken Sie in Agent > **Agents bereitstellen** auf die Schaltfläche **Gemeinsam nutzen** neben dem `Default Install`-Paket.
2. Aktivieren Sie **Anderen Benutzern Änderungen gestatten**.
3. Klicken Sie auf **Speichern**.
4. Klicken Sie auf das Bearbeitungssymbol neben dem `Default Install`-Paket.

Wenn Sie das `Default Install`-Paket bearbeiten, ist die Schaltfläche **Speichern** aktiviert.

Hinweis: Falls Sie das `Default Install`-Paket löschen, wird es sofort neu erstellt.

Agent-Einstellungen konfigurieren

Agent-Einstellungen

Agent-Einstellungen bestimmen das Verhalten des Agents auf dem verwalteten Rechner. Obgleich jeder Agent einzeln konfiguriert werden kann, wird das Verwalten von Rechnern vereinfacht, wenn Sie ähnliche Einstellungen für jeden Typ von verwaltetem Rechner festlegen. So können beispielsweise für Laptops, Desktops und Server Einstellungen festgelegt werden, die typisch für diesen Rechnertyp sind. Entsprechend können auch die Rechner eines Kunden eindeutige Merkmale aufweisen, die sich von denjenigen auf Rechnern anderer Kunden unterscheiden. Zu den Agent-Einstellungstypen zählen:

- **Anmeldedaten** *(siehe 77)*
- **Agent-Menü** *(siehe 66)*
- **Check-in-Kontrolle** *(siehe 68)*
- **Arbeitsverzeichnis** *(siehe 72)*
- **Protokolle** *(siehe 36)*
- **Profil bearbeiten** *(siehe 73)*
- **Sammlungen ansehen** *(siehe 628)*
- **Portalzugriff** *(siehe 75)*
- Remote-Control-Richtlinie
- **Patch-Einstellungen** *(siehe 624)*
- Patchdateiquelle
- Zugehörigkeit zu Patch-Richtlinien
- **Meldungen** *(siehe 284)*
- **Ereignisprotokoll-Meldungen** *(siehe 316)*
- **Monitor-Sets** *(siehe 267)*
- **Dateien verteilen** *(siehe 135)*
- **Geplante Agent-Verfahren** *(siehe 92)*

Richtlinien im Vergleich zu Vorlagen

Es gibt zwei allgemeine Methoden für die Verwaltung von Agent-Einstellungen auf mehreren

Rechnern.

- **Konfigurieren von Agent-Einstellungen mit Richtlinien** *(siehe 46)* – Dies ist die bevorzugte *dynamische* Methode für die Verwaltung von Agent-Einstellungen auf Hunderten, wenn nicht sogar Tausenden von Rechnern. Sobald eine Richtlinie auf einen Zielrechner angewendet wird, erfolgt die Übertragung automatisch.
- **Konfigurieren von Agent-Einstellungen mit Vorlagen** *(siehe 46)* – Dies ist die veraltete *statische* Methode für die Verwaltung von Agent-Einstellungen auf mehreren Rechnern. Agent-Einstellungen müssen bei jeder Änderung manuell auf die jeweiligen Zielrechner kopiert werden.

Konfigurieren von Agent-Einstellungen mit Richtlinien

Das **Policy Management**(KPM)-Modul im VSA verwaltet *Agent-Einstellungen nach Richtlinie*. Sobald den Rechnern, Rechnergruppen oder Organisationen Richtlinien zugewiesen wurden, *werden diese automatisch übertragen*, ohne dass der Benutzer weiter eingreifen muss.

Der Systemmanagement-Assistent

Es befindet sich ein Richtlinieninstallationsassistent auf der Registerkarte System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Systemmanagement.

Mit dem Einrichtungsassistenten können Sie schnell *Rechnerverwaltungsrichtlinien für eine bestimmte Organisation konfigurieren und anwenden.* Sind die Richtlinien konfiguriert, werden diese auf alle Rechner angewandt, die Sie im Auftrag der betreffenden Organisation verwalten. Richtlinien bestimmen viele verschiedene Aspekte der Rechnerverwaltung:

- Audit-Planung
- Monitoring
- Benachrichtigungen
- Patch-Verwaltung
- Rechner-Routinewartung mithilfe von Agentverfahren

Dank der Richtlinien müssen Sie nicht mehr jeden Rechner einzeln verwalten. Sie müssen nur eine Richtlinie zuweisen oder ändern. Eine Richtlinienzuweisung oder -änderung im Rahmen einer zugewiesenen Richtlinie wird innerhalb von 30 Minuten an alle beteiligten Rechner verteilt, ohne dass Sie in die Planung eingreifen müssen. Danach können Sie leicht feststellen, ob ein verwalteter Rechner die zugewiesenen Richtlinien erfüllt oder nicht. Die Verfolgung der Erfüllung jeder einzelnen Richtlinie liefert Ihnen die Informationen, die Sie für die zuverlässige Bereitstellung von IT-Diensten für die gesamte von Ihnen betreute Organisation benötigen.

> **Hinweis:** Eine detaillierte Erklärung jeder Option im **Installationsassistenten** *(http://help.kaseya.com/webhelp/DE/SSP/7000000/index.asp#11220.htm)* finden Sie im **Standard Solution Package**.

Konfigurieren von Agent-Einstellungen mit Vorlagen

Rechner-ID-Vorlagen

Eine Rechner-ID-Vorlage ist ein *Rechner-ID-Datensatz ohne Agent*. Da sich ein Agent niemals an einem Rechner-ID-Vorlagenkonto anmeldet, wird er nicht in die Gesamtzahl Ihrer Lizenzen eingerechnet. Sie können kostenlos so viele Rechner-ID-Vorlagen erstellen, wie Sie wünschen. Beim Erstellen eines Agent-Installationspakets werden die Paketeinstellungen normalerweise von einer ausgewählten Rechner-ID-Vorlage kopiert. Für gewöhnlich werden Rechner-ID-Vorlagen für bestimmte Rechnertypen erstellt und konfiguriert. Rechnertypen umfassen Desktops, Autocad, QuickBooks, Small-Business-Server, Exchange-Server, SQL-Servers usw. **Basierend auf der von Ihnen definierten Rechner-ID-Vorlage kann ein entsprechendes Installationspaket erstellt werden.**

- Erstellen Sie Rechner-ID-Vorlagen über Agent > **Erstellen** *(siehe 55)*.
- Importieren Sie eine Rechner-ID-Vorlage über Agent **Import/Export** *(siehe 64)*.

- Erstellen Sie ein Agent-Installationspaket basierend auf einer Rechner-ID-Vorlage über Agent > **Agents bereitstellen** *(siehe 40)*.
- Kopieren Sie *ausgewählte* Einstellungen von Rechner-ID-Vorlagen auf vorhandene Rechner-ID-Konten über Agent > **Einstellungen kopieren** *(siehe 62)*.
- Bestimmen Sie die Gesamtzahl der Rechner-ID-Vorlagenkonten in Ihrem VSA über System > **Statistiken** *(siehe 442)*.
- Konfigurieren Sie Einstellungen für die Rechner-ID-Vorlage mithilfe der Standard-VSA-Funktionen, genau wie Sie ein Rechner-ID-Konto ohne Agent konfigurieren würden.
- Für Windows-, Apple- und Linux-Rechner werden separate Rechner-ID-Vorlagen empfohlen. Alternativ können Sie ein Paket erstellen, das das entsprechende Betriebssystem automatisch auswählt und Einstellungen von einer Vorlage kopiert, die ein Agent-Verfahren mit bestimmten Schritten das für das jeweilige Betriebssystemt enthält.

So wenden Sie eine Rechner-ID-Vorlage auf ein Paket an:

1. Legen Sie mithilfe des **Paket erstellen**-Assistenten in **Agent bereitstellen** die Vorlage als die Quellrechner-ID fest, von der die Einstellungen kopiert werden sollen, wenn Sie das zu installierende Paket erstellen.
2. Fügen Sie mithilfe des gleichen Assistenten Attribute zu dem Paket hinzu. Diese zusätzlichen Attribute sind für gewöhnlich von Kunde zu Kunde verschieden und sollten daher nicht in der Vorlage gespeichert werden.

Agent-Einstellungen kopieren

Rechner-ID-Vorlagen *(siehe 627)* werden anfänglich dazu verwendet, um ein Agent-Installationspaket zu erstellen. Dabei wird die Vorlage als Quelle verwendet, um Einstellungen zu kopieren. Aber selbst nach der Installation der Agents auf verwalteten Rechnern müssen Sie die Einstellungen auf vorhandenen Rechner-ID-Konten aktualisieren, da sich die Anforderungen Ihrer Kunden ändern und Sie sich immer besser mit dem VSA auskennen. Verwenden Sie in diesem Fall Agent > **Einstellungen kopieren**, um diese Änderungen auf alle Rechner-IDs zu kopieren, für die Sie Zugriffsberechtigungen haben. Achten Sie darauf, `Do Not Copy` für jede Einstellung auszuwählen, die Sie nicht überschreiben möchten. Verwenden Sie `Add`, um Einstellungen zu kopieren, ohne vorhandene Einstellungen zu entfernen. Kaseya empfiehlt, zuerst die Änderungen an einer ausgewählten Vorlage vorzunehmen und diese Vorlage dann als Quellrechner-ID zum Kopieren zu verwenden. Auf diese Weise wird sichergestellt, dass Ihre Rechner-ID-Vorlagen die "Master-Repositories" aller Ihrer Agent-Einstellungen bleiben und als Quelle für die Agent-Installationspakete und vorhandenen Rechner-ID-Konten dienen können.

Vorlagen und gefilterte Ansichten

Es besteht eine sinngemäße Beziehung zwischen den Rechner-ID-Vorlagen und dem Filtern Ihrer Ansicht von ausgewählten Rechnern mit der Ansichtdefinitionsoption **Nur ausgewählte Rechner-IDs anzeigen**. (Ansichtsdefinitionen werden in Arbeiten mit Agents im VSA) beschrieben.) Beim Definieren einer Rechner-ID-Vorlage namens "Laptops" ist es beispielsweise einfacher, Einstellungen auf alle "Laptops" anzuwenden, für die Ihrer Verantwortung unterliegen, wenn Sie eine gefilterte Ansicht mit Namen "Laptops" besitzen. Wählen Sie ganz einfach die Ansicht für "Laptops" aus. Daraufhin werden auf jeder Funktionsseite nur Laptops angezeigt, egal zu welcher Rechnergruppe sie gehören. Entsprechendes gilt auch für "Desktops", "Workstations", Exchange-Server" usw.

Gefilterte Ansichten ausgewählter Rechner sind besonders dann nützlich, wenn Sie die Einstellungen von einer Rechner-ID-Vorlage mithilfe der oben beschriebenen Funktion **Einstellungen kopieren** auf bestehende Agents kopieren möchten.

Basis-Vorlagen und Inventarisierungen

Da Sie sich nie ganz sicher sein können, welche Einstellungen auf einen Rechner angewendet werden sollten, bis Sie eine Inventarisierung dieses Rechners durchführen, sollten Sie ein Agent-Paket installieren, das von einer "Basis"-Vorlage erstellt wurde, auf der die meisten Agent-Einstellungen *deaktiviert* sind. Sobald Sie die Inventarisierung durchgeführt haben, können Sie entscheiden, welche

Einstellungen auf welchen Rechner angewendet werden sollen. Mit der Funktion **Einstellungen kopieren** können Sie Einstellungen von der entsprechenden Vorlage auf den neuen Agent kopieren.

Befehlszeilenschalter für Agent-Installation

In Befehlszeilenschaltern für Agent-Installationen für `KcsSetup` muss weder die Groß-/Kleinschreibung noch die Reihenfolge beachtet werden. Trennen Sie die Schalter durch eine Leerstelle. Zum Beispiel: `KcsSetup /e /g=root.unnamed /c`

> **Hinweis:** Bei Apple-Agents können Befehlszeilenschalter nur für die Erstellung des Agent-Installationspaketes verwenden werden.

`/b` – Das System wird nach Abschluss der Installation neu gestartet. Die Agent-Installation erfordert einen Neustart, damit die Treiber geladen werden können. Verwenden Sie diesen Schalter bei Paketen, die Benutzern gegeben wurden, die keine Rechte zum Abschalten des Rechners haben.

`/c` – Verwendet den Computernamen als Rechner-ID für das neue Konto. Falls der Computername nicht durch das Programm festgestellt werden kann, wird der Rechnerbenutzer zur Eingabe einer Rechner-ID aufgefordert. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation angehalten und ein Fehler im Installationsprotokoll verzeichnet.

`/d` – Verwendet den aktuellen Domänennamen als Gruppen-ID für das neue Konto. Falls der Domänenname nicht durch das Programm festgestellt werden kann, wird der Rechnerbenutzer zur Eingabe der Gruppen-ID aufgefordert. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation angehalten und ein Fehler im Installationsprotokoll verzeichnet.

`/e` – Die Installation wird sofort beendet, wenn das Installationsprogramm ermittelt, dass bereits ein Agent installiert ist. Verwenden Sie `/e` am Ende der Anmeldeverfahren. `/k` oder `/r` überschreibt `/e`.

`/f "Publisher"` – Gibt den vollen Namen des Dienstanbieters oder Tenant an. Nur Windows.

`/g=xxx` – Gibt die Gruppen-ID für das neue Konto an. `xxx` muss eine alphanumerische Zeichenfolge sein und darf keine Leerstellen oder Satzzeichen enthalten.

`/h` – Zeigt den Hilfedialog an, der alle Befehlszeilenschalter auflistet, es sei denn, der Schalter `/s` ist eingestellt. In diesem Fall wird die Anwendung beendet.

`/i` – Nicht kritische Fehler, z. B. falsche oder unbestimmte Versionen von WinSock2 oder unbestimmte Versionen des Betriebssystems werden ignoriert und das Fortsetzen der Installation wird erzwungen.

`/j` – Es wird kein Agent-Shortcut zum Menü **Start > Alle Programme** installiert. Nur Windows.

`/k` – Der Benutzer wird über ein Dialogfeld gefragt, ob eine Neuinstallation OK ist, wenn der Agent bereits auf dem Rechner ermittelt wurde. Ohne diesen Schalter wird das Installationsprogramm beendet, falls ein Agent bereits vorhanden ist.

`/m=xxx` – Gibt die Rechner-ID für das neue Konto an. `xxx` muss eine alphanumerische Zeichenfolge sein und darf keine Leerstellen oder Satzzeichen enthalten.

`/n = partitionId` – Gibt die Partition-ID der **Tenant-Partition** *(siehe 631)* an, zu der das installierte Agent-/Rechner-ID-Konto gehört.

`/o "Company Title"` – Gibt den Firmentitel des Dienstanbieters oder Tenant an. Nur Windows.

`/p "install_path"` – Überschreibt den Standard-Installationspfad, indem der vollständige Verzeichnispfad (einschließlich des Laufwerksbuchstabens) angegeben wird, in dem der Agent installiert werden soll.

- Unter Windows erstellt die Agent-Installation standardmäßig ein Verzeichnis unter Verwendung des `%ProgramFiles%`-Variablenpfads als `\<company>\<Agent-Instance-Guid>`.
- Unter Linux erstellt die Agent-Installation standardmäßig ein Verzeichnis mit dem Namen `/opt/Kaseya/<Agent-Instance-Guid>`.
- Unter Apple wird der /p-Schalter nicht unterstützt und ignoriert.

`/r` – Führt das Installationsverzeichnis aus und installiert den Agent neu, selbst wenn bereits ein Agent

auf dem Rechner vorhanden ist.

`/s` – Die Installation wird im automatischen Modus ausgeführt. Alle Dialogfelder werden unterdrückt.

`/t "Title"` – Gibt den Titel jedes Dialogfeldes an, das dem Benutzer während der Installation angezeigt wird. Der Standardtitel lautet: `"Kaseya Agent"`.

`/u` – Verwendet den aktuellen Rechnerbenutzernamen als Rechner-ID für das neue Konto. Falls der Rechnerbenutzername nicht durch das Programm festgestellt werden kann, wird der Benutzer zur Eingabe einer Rechner-ID aufgefordert. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation angehalten und ein Fehler im Installationsprotokoll verzeichnet.

`/v` – Ordnet diesen Agent einem bestehenden Agent-Konto im VSA zu, wenn Rechnername, Agent-Name und Organisation die gleichen für die gleiche Partition sind. Ignoriert das Erstellen eines neuen Agent-Kontos, wenn eine MAC-Adresse ermittelt wird. Geeignet für die Wiederverwendung von vorhandenen Agent-Konten, die für rückgängig gemachte VDI-Ressourcen erstellt wurden.

`/w` – Überschreibt die vorhandene Konfigurationsdatei mit einer in der Agent-Installation enthaltenen Konfigurationsdatei. Verwenden Sie dies mit dem Schalter `/r`, um einen Agent mit neuen Servereinstellungen zu installieren. Dies ist für einen bestehenden Agent beabsichtigt, der versucht, eine Verbindung mit einem nicht mehr existierenden Server herzustellen.

`/x` – Deaktiviert die Fernsteuerung, nachdem der Agent erfolgreich installiert wurde. Bei einer Aktualisierung oder Neuinstallation wird diese Option ignoriert. Die Fernsteuerung dieses Rechners kann erst erfolgen, wenn der Benutzer **Fernsteuerung aktivieren** auswählt, indem er mit der rechten Maustaste auf das K-Symbol in der Systemablage klickt.

`/z “Message”` – Gibt die Meldung an, die dem Benutzer nach Abschluss der Installation angezeigt wird. Die Ausnahme bildet der automatische Modus (`/s`). In diesem Fall wird die Installation abgeschlossen und die Statusmeldung in das Installationsprotokoll geschrieben. Die Standardmeldung lautet: "`The Agent has been installed successfully on your computer.`”

`/?` – Zeigt den Hilfedialog an, der alle Befehlszeilenschalter auflistet, es sei denn, der Schalter `/s` ist eingestellt. In diesem Fall wird die Anwendung beendet. Nur Windows.

Installationsschalter nur für Linux

Siehe **Installation von Linux-Agents** *(siehe 52)*.

Probleme und Fehler bei der Installation

Beim Installieren von Agents können die folgenden Probleme und Fehlschläge eintreten:

- **Ungültige Anmeldedaten** – Die an das Paket gebundenen **Anmeldedaten** *(siehe 614)* müssen über Administratorrechte auf dem lokalen Rechner verfügen. Der Agent wird als Systemdienst installiert und benötigt volle Benutzerberechtigungen, um erfolgreich installiert werden zu können. Der Administratorname kann ein Domänenbenutzer der Form `domain\administrator` oder `administrator@domain` sein. Stellen Sie bei Vista, 7 und 2008 Rechnern sicher, dass die Benutzerkontensteuerung (UAC) deaktiviert ist, damit Administrator-Anmeldedaten verwendet werden können.
- **Angegebene Domäne für einen Rechner ist nicht die Domäne** – Falls in Schritt 2 der Paketerstellung in **Agent bereitstellen** die Option **Domänenname** ausgewählt wird und der Computer nicht Teil einer Domäne ist, setzt ein Installationspaket den Prozessor bei 100 % fest. Es wird jedoch schließlich installiert.
- **Durch Anti-Virus-Programm blockiert** – Manche Anti-Virus-Programme können die Agent-Installation als Sicherheitsbedrohung klassifizieren und ihre Ausführung blockieren.
- **Durch Sicherheitsrichtlinie blockiert** – Lokale oder Domänen-Sicherheitsrichtlinien können den Zugriff auf das Installationsverzeichnis (normalerweise das Verzeichnis `Program Files`) verhindern.
- **Ungenügende Lizenzen** – Falls nicht genügend VSA-Lizenzen verfügbar sind, kann der Agent daran gehindert werden, sich zum ersten Mal anzumelden und ein Konto zu erstellen. Sollte dies geschehen, wird nach der Installation des Agents auf dem Rechner ein graues K-Symbol in der

Systemablage angezeigt, das niemals zu blau wechselt. Wenn der Cursor auf das graue Agent-Symbol gesetzt wird, meldet ein angezeigter Tooltip "'Rechner-ID.Gruppen-ID' nicht vom Kaseya Server erkannt".

Apple

- Macintosh Agents können nicht ohne einen gültigen Benutzernamen und gültiges Kennwort bereitgestellt werden.

Mehrere Agents installieren

Es können mehrere Agents auf dem gleichen verwalteten Rechner installiert werden, wobei sich jeder bei verschiedenen Kaseya Servers anmeldet. *Führen Sie das v6-Agent-Installationsprogramm von einem anderen Kaseya Server* aus und Sie erhalten einen zusätzlichen Agent.

- Gilt für Windows- und Linux-Agents. Die Installation mehrerer Macintosh-Agents wird nicht unterstützt.
- Ein v6-Agent kann mit anderen v6-Agents koexistieren.
- Nur für Windows:
  - Ein v6-Agent kann mit v5.1- oder älteren Agents koexistieren.
  - Jeder verwaltete Rechner mit einem Domain-Controller-Anmeldeverfahren, auf dem das Agent-Installationsverfahren automatisch ausgeführt wird, *muss* die Datei `KcsSetup` aus der v5.1-Version oder einer älteren Version mit dem v6-Agent aktualisieren. Das v5.1- oder ältere Installationsprogramm erkennt den neueren v6-Agent nicht und wird neu installiert, selbst wenn der v6-Agent vorhanden ist.

Treibernutzung – nur Windows-Agents

Wenn mehrere Agents auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 83)*, **Netzwerkzugriff** *(siehe 84)* und **Anwendungsblocker** *(siehe 88)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese Treiber kontrolliert.

- Die Treiber werden ursprünglich vom zuerst installierten Agent kontrolliert.
- Wenn der erste Agent, der die Treiber kontrolliert, deinstalliert wird, werden diese Treiber ebenfalls deinstalliert und diese drei Funktionen können von keinem Agent mehr ausgeführt werden.
- Diese Treiber werden durch eins der folgenden Ereignisse neu installiert:
  - Einer der vorhandenen Agents auf dem Rechner wird aktualisiert. Der aktualisierte Agent übernimmt die Kontrolle über die Treiber und kann diese drei Funktionen ausführen.
  - Ein neuer Agent wird installiert. Der neu installierte Agent übernimmt die Kontrolle über die Treiber und kann diese drei Funktionen ausführen.
- Informationen darüber, wie Sie ermitteln, welcher Agent die Kontrolle über die Treiber hat, finden Sie unter *Registrierung* weiter unten.

Agents auf verwalteten Rechnern identifizieren

Bei der Installation eines Kaseya-Agents wird ein *eindeutiger Identifikator* für ihn erstellt, der aus der 6-stelligen Kunden-ID des Kaseya Server und einer willkürlich erzeugten 14-stelligen Zahl besteht. Dieser eindeutige Identifikator wird als Agent-GUID bezeichnet. Er wird dazu verwendet, separate Unterordner zum Speichern von Agent-Programmdateien zu erstellen, und dient als Unterschlüssel für Agent-Registrierungswerte.

In den unten stehenden Beispielen zeigen Agents spezifische Informationen über die folgenden Platzhalter an:

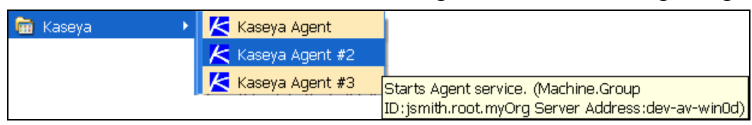
- `<GUID>` – Die Agent-Instanz GUID.
- `<company>` – Das Installationsverzeichnis des Agents

- `<serveraddress>` – Die Kaseya Server-Adresse, bei der sich der Agent anmeldet.
- `<machineID.groupID.orgID>` – Die Rechner-ID, Gruppen-ID und Organisations-ID des Agents auf dem Kaseya Server.
- `<shortcutname>` – Der Name des Shortcut. Beispiel: `Kaseya Agent #2`.

Shortcuts

Wenn Sie den Mauszeiger über einem Shortcut für einen Kaseya-Agent bewegen, z. B. ein Shortcut im Windows-Startmenü, zeigt ein Tooltip Folgendes an:

- `Start Agent service. (machine.GroupID:<machineID.groupID.orgID> Address:<serveraddress>)`
- Wenn Sie mit der rechten Maustaste auf einen Shortcut klicken, wird dieser Text ebenfalls im Kommentarfeld der Shortcut-Eigenschaftsseite angezeigt.



Info zu Agent

Klicken Sie mit der rechten Maustaste auf das K-Symbol in der Systemablage eines verwalteten Rechners und wählen Sie die Option **Info zu Agent** aus, um die folgenden Informationen anzuzeigen:

- Agentversion
- Serveradresse – `<serveraddress>`
- Produkt-ID – `<GUID>`
- Programmtitel – `<shortcutname>`

Windows-Agents

Hinzufügen/Entfernen

Agents werden folgendermaßen angezeigt:

- `Kaseya Agent (<machineID.groupID.orgID> - <serveraddress>)`
- `Kaseya Agent #2 (<machineID.groupID.orgID> - <serveraddress>)`
- `Kaseya Agent #3 (<machineID.groupID.orgID> - <serveraddress>)`

Dienste

Im Beschreibungsfeld des Dienstes wird derselbe Text wie im oben stehenden Agent-Shortcut angezeigt.

Registry

Die Registrierungseinstellungen des Agents werden folgendermaßen angezeigt:

```
HKLM\Software\Kaseya\Agent
   DriverControl - The agent that controls driver usage.
   KES_Owned_By - The agent that manages the KES client.

HKLM\Software\Kaseya\Agent\<GUID>
   Title - <shortcutname>
   Path - C:\Program Files\<company>\<GUID>
   ServAddr - <serveraddress>
   machineID - <machineID.groupID.orgID>
   DriverControl - The agent that controls driver usage.
   KES_Owned - The agent that manages the KES client.
```

Standard-Agent-Installationsordner

- Siehe den `/p`-Schalter in **Befehlszeilenschalter für Agent-Installation** *(siehe 48)*.

Installation von Linux Agents

> **Hinweis:** Siehe **Systemvoraussetzungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)* für Angaben zu unterstützten Linux-Betriebssystemen und Browsern.

Manuelle Installation von Linux Agents

1. Öffnen Sie einen Firefox oder Chrome Browser auf Ihrem Linux Rechner in einer Gnome-Sitzung und melden Sie sich am VSA an.
2. Zeigen Sie die Seite Agent > Agents installieren > **Agents verteilen** *(siehe 40)* an.
3. Klicken Sie auf den Hyperlink **Hier klicken um Standard-Agent herunterzuladen** und starten Sie den Download des Standard-Agent-Installationspaketes. Ein Linux Agent-Installationspaket wird heruntergeladen.

   > **Hinweis:** Alternativ können Sie Ihr eigenes Linux-Paket erstellen, indem Sie auf **Paket erstellen** drücken und sich durch den Installationsassistenten führen lassen.

4. Wenn der Download vollständig ist, suchen Sie die Datei `KcsSetup.sh` im Download-Verzeichnis des Linux Rechners.

   > **Hinweis:** Wenn Sie `KcsSetup.exe` oder `KcsSetup.zip` heruntergeladen haben, haben Sie die falsche Installationsdatei heruntergeladen, weil das ausgewählte Installationspaket nur für Windows oder Macintosh gilt.

5. Führen Sie die folgenden Befehle als Stammverzeichnis aus:
   ```
   # chmod +x KcsSetup.sh
   # ./KcsSetup.sh
   ```
   Der Agent wird installiert und startet. Melden Sie sich am VSA an und prüfen Sie den Agent-Status.
   Weitere Informationen finden Sie in der Installationsprotokolldatei unter:
   `/tmp/KASetup_<pid>.log`
   , wobei <pid> die Prozess-ID der `./KcsSetup.sh`-Ausführung ist.

   > **Hinweis:** Führen Sie `KcsSetup.sh -V -D` für Verbose-Terminalausgabe aus.

> **Hinweis:** Führen Sie `KcsSetup.sh -X` aus, um die in der /tmp-Datei erstellten temporären Dateien auszuführen. Das Speichern dieser Dateien ist nützlich, wenn eine fehlgeschlagene Installation behoben wird.

6. Nachdem der Linux-Agent installiert ist, melden Sie sich an und wieder ab, damit Sie das Kaseya Agent-Symbol im Gnome-Panel sehen.

Installation von Linux Agents über LAN-Watch und Agents installieren

1. Planen Sie einen Discovery > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*-Scan und *nutzen Sie dafür einen bestehenden Linux-Agent als Ermittlungsrechner*.
2. Installieren Sie einen Linux-Agent auf einem ermittelten Linux-Rechner mit einer der Discovery > Ermittelte Geräte-Seiten.
   - Geben Sie `root` in das Feld **Admin-Anmeldung** ein.
   - Geben Sie das Kennwort für den `root`-Benutzer der anvisierten Linux Rechner im Feld **Kennwort** ein.
   - Wählen Sie ein Agent-Installationspaket aus dem Feld **Agent-Paket zur Installation wählen** aus.
   - Kreuzen Sie die Kontrollkästchen neben einem oder mehreren anvisierten Linux Rechnern an oder geben Sie die IP-Adresse oder den Namen des anvisierten Linux Rechner in das Feld **nicht gefundener Rechner** ein.
   - Klicken Sie auf die Schaltfläche **Abschicken**.

> **Hinweis:** Die Seite **Agents installieren** unterscheidet aktuell nicht zwischen Linux und anderen Systemen. Die Person, die den Agent installiert, muss darauf achten, dass nur Linux Systeme ausgewählt werden.

Einen Linux Agent manuell deinstallieren

Ein `<install-dir>/bin/KcsUninstaller` wird immer mit dem Agent installiert und entfernt den Agent. Agents werden üblicherweise in das Verzeichnis `/opt` installiert.

Führen Sie die folgenden Befehle als Stammverzeichnis aus:

```
# ./KcsUninstaller
```

> **Hinweis:** Führen Sie den Befehl `./KcsUninstaller -D -V` aus, um den Agent mit Verbose-Terminalausgabe zu deinstallieren.

Fehlerbehebung bei Linux-Agent-Installationen

- Siehe die Community-Seite **Fehlerbehebung bei Linux-Agent-Installationen** *(https://helpdesk.kaseya.com/entries/36223968)*.

Unterstützte Linux Funktionen

Linux Agents unterstützen die folgenden Funktionen:

- Agent-Verfahren
- Letzte Audits, Basis-Audits und System-Audits
- Remote Control und FTP mit VNC
- SSH
- Kennwort zurücksetzen
- LAN-Watch und Agents installieren – Siehe **Linux Agents installieren** *(siehe 52)*.
- Meldungen
- Überwachung der Prozesse

- Überwachung von SNMP
- Log-Parser
- Benutzerspezifische Site-Anpassung – Die Registerkarte **Agent-Symbole** bietet jetzt einen Symbolsatz für Linux Agents, die Sie anpassen können.
- Nur auf bestimmte nicht-pluginfähige Elemente kann über einen Linux-basierten Browser oder beim Browsen auf einen Linux Agent-Rechner zugegriffen werden. Dazu gehören:
- Live-Connect – Nur auf bestimmte nicht-pluginfähige Elemente kann über einen Linux-basierten Browser oder beim Browsen auf einen Linux Agent-Rechner zugegriffen werden. Unterstützte Menüoptionen wie folgt:
  - Startseite
  - Agent-Daten
  - Audit-Information
  - Ticketing (oder Service-Desk-Ticketing)
  - Chat
  - Video-Chat

Siehe **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Unterstützte Apple-Funktionen

Apple-Agents unterstützen die folgenden Funktionen:

- Audits – Ausgewählte Hardware- und Software-Attribute
- Agent-Verfahren
- Remote Control
- FTP
- SSH
- Kennwort zurücksetzen
- Task-Manager
- Live-Connect mit Desktopzugriff.
  - Auf Apple Leopard (Intel) und höher, einschließlich Lion und Mountain Lion, können Sie Desktopzugriff in Live-Connect nutzen, um ein Windows System, das Firefox oder Safari verwendet, remote zu steuern.
  - Unter Verwendung einer unserer unterstützten Browser können Sie unter Windows Desktop-Zugriff verwenden, um Apple Leopard (Intel) und höher, einschließlich Lion und Mountain Lion, remote zu steuern.
- Aufzeichnung der Desktop-Sitzung über Fernsteuerung und Schnellansicht für Snow Leopard und höher, einschließlich Lion und Mountain Lion.
- LAN-Watch über Ermittlung
- Monitoring wurde unterstützt:
  - SNMP-Monitoring
  - Monitoring in Monitor-Sets verarbeiten
  - Systemprüfung
  - Log-Parser

Siehe **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Erstellen

Agent > Agents installieren > Erstellen

Auf der Seite **Erstellen** werden ein Rechner-ID-Konto und Agent-Installationspaket für einen *einzigen* Rechner erstellt. Sie erstellen zuerst das Rechner-ID-Konto und dann ein Installationspaket für den Rechner. Normalerweise gilt die Seite **Erstellen** für Folgendes:

- **Rechner-ID-Vorlagen** – In diesem Fall braucht kein Installationspaket erstellt zu werden, da **Rechner-ID-Vorlagen** *(siehe 627)* nicht zur Installation auf einem Rechner gedacht sind.
- **Neuinstallieren von Agents für ein vorhandenes Konto** – Da die Installationspakete **Erstellen** *nicht automatisch ein neues Rechner-ID-Konto erstellen*, können Sie die Seite **Erstellen** verwenden, um Agents auf verwalteten Rechnern für *vorhandene* Konten *neu zu installieren*.
- **Gesicherte Umgebungen** – Gesicherte Umgebungen erfordern eventuell eine manuelle Einrichtung jedes Rechners. Vielleicht müssen Sie beispielsweise ein neues Rechner-ID-Konto manuell benennen und/oder ein Agent-Installationspaket mit eindeutigen Anmeldedaten für einen einzelnen Rechner erstellen. Ein Benutzer muss lokal bei einem Zielrechner angemeldet sein, um das Paket zu installieren.

> **Hinweis:** Verwenden Sie Agent > **Agents erstellen** *(siehe 40)*, um Agent-Installationspakete zu erstellen und auf *verschiedenen* Rechnern zu installieren. Das Installationspaket **Agents bereitstellen** *erstellt automatisch ein Rechner-ID-Konto*, wenn es installiert wird. Dazu muss jedoch die automatische Kontenerstellung über System > **Check-in Policy** *(siehe 405)* aktiviert worden sein.
>
> **Hinweis:** Verwenden Sie **Discovery**, um Agents auf *Remote-Systemen* zu installieren.

Rechner-IDs vs. Agents

Bei der Erläuterung von Agents ist es nützlich, zwischen der **Rechner-ID/Gruppen-ID/Organisations-ID** *(siehe 626)* und dem **Agent** *(siehe 611)* zu unterscheiden. Die Rechner-ID/Gruppen-ID/Organisations-ID ist der **Kontoname** für einen verwalteten Rechner in der VSA-Datenbank. Der Agent ist die Clientsoftware, die auf dem verwalteten Rechner installiert ist. Zwischen dem Agent auf einem verwalteten Rechner und seinem Kontonamen auf dem VSA besteht eine Eins-zu-Eins-Beziehung. Die Agent-Aktionen auf dem verwalteten Rechner werden von den Aufgaben geleitet, die einer Rechner-ID von VSA-Benutzern zugewiesen wurden.

Agent-Lizenzzahlen

Die folgenden Ereignisse wirken sich auf Agent-Lizenzzahlen aus:

- Eine "nicht verwendete" Agent-Lizenz wird in "verwendet" geändert, wenn ein Rechner-ID-Konto erstellt und der Agent installiert wird.
- Falls der Agent, aber nicht das Konto, gelöscht wird, wird die Agent-Lizenz dennoch als "verwendet" betrachtet.
- Wenn das Konto gelöscht wird (ungeachtet dessen, was mit dem Agent geschieht), erhält die Agent-Lizenz wieder den Status "nicht verwendet".
- Falls ein Konto erstellt wird, der Agent jedoch noch nicht zum ersten Mal installiert ist, wird das Konto als **Rechner-ID-Vorlage** *(siehe 627)* bezeichnet. Rechner-ID-Kontovorlagen werden erst als "verwendet" gezählt, wenn Sie den Agent installieren.

Anmeldedaten in Agent-Installationspakete einschließen

Gegebenenfalls kann ein Agent-Installationspaket erstellt werden, das **Anmeldedaten** *(siehe 614)* eines Administrators für den Zugriff auf ein Kundennetzwerk enthält. Anmeldedaten sind nur erforderlich, wenn Benutzer Pakete auf Rechnern installieren und *keinen Administratorzugriff* auf ihr Netzwerk haben. Die Anmeldedaten des Administrators sind verschlüsselt, niemals als Klartext verfügbar und an das Installationspaket gebunden.

Auswahl des Betriebssystems

Agent-Pakete können erstellt werden, um Agents auf Rechnern zu installieren, auf denen Windows-, Apple- oder Linux-Betriebssysteme laufen. Es kann jedoch auch automatisch das Betriebssystem des Rechners, der den Agent herunterlädt, gewählt werden.

Rechner-ID-Vorlagen

Eine Rechner-ID-Vorlage ist ein *Rechner-ID-Datensatz ohne Agent*. Da sich ein Agent niemals an einem Rechner-ID-Vorlagenkonto anmeldet, wird er nicht in die Gesamtzahl Ihrer Lizenzen eingerechnet. Sie können kostenlos so viele Rechner-ID-Vorlagen erstellen, wie Sie wünschen. Beim Erstellen eines Agent-Installationspakets werden die Paketeinstellungen normalerweise von einer ausgewählten Rechner-ID-Vorlage kopiert. Für gewöhnlich werden Rechner-ID-Vorlagen für bestimmte Rechnertypen erstellt und konfiguriert. Rechnertypen umfassen Desktops, Autocad, QuickBooks, Small-Business-Server, Exchange-Server, SQL-Servers usw. **Basierend auf der von Ihnen definierten Rechner-ID-Vorlage kann ein entsprechendes Installationspaket erstellt werden.**

- Erstellen Sie Rechner-ID-Vorlagen über Agent > **Erstellen** *(siehe 55)*.
- Importieren Sie eine Rechner-ID-Vorlage über Agent **Import/Export** *(siehe 64)*.
- Erstellen Sie ein Agent-Installationspaket basierend auf einer Rechner-ID-Vorlage über Agent > **Agents bereitstellen** *(siehe 40)*.
- Kopieren Sie *ausgewählte* Einstellungen von Rechner-ID-Vorlagen auf vorhandene Rechner-ID-Konten über Agent > **Einstellungen kopieren** *(siehe 62)*.
- Bestimmen Sie die Gesamtzahl der Rechner-ID-Vorlagenkonten in Ihrem VSA über System > **Statistiken** *(siehe 442)*.
- Konfigurieren Sie Einstellungen für die Rechner-ID-Vorlage mithilfe der Standard-VSA-Funktionen, genau wie Sie ein Rechner-ID-Konto ohne Agent konfigurieren würden.
- Für Windows-, Apple- und Linux-Rechner werden separate Rechner-ID-Vorlagen empfohlen. Alternativ können Sie ein Paket erstellen, das das entsprechende Betriebssystem automatisch auswählt und Einstellungen von einer Vorlage kopiert, die ein Agent-Verfahren mit bestimmten Schritten das für das jeweilige Betriebssystemt enthält.

Vordefinierte Meldungen

Wenn Sie über Agent > **Erstellen** ein Rechner-ID-Konto erstellen *und Einstellungen nicht von einem anderen Rechner kopieren*, werden verschiedene typische Benachrichtungen für das Rechner-ID-Konto standardmäßig erstellt.

Neue Konten-Einstellungen kopieren aus

Klicken Sie auf ein Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID. Agent-Einstellungen werden von dieser Rechner-ID kopiert.

> **Hinweis:** Wenn Sie keine Rechner-ID angeben, von der kopiert werden soll, und auf **Erstellen** klicken, wird ein neues, verwendbares Rechner-ID-Konto mit den Kaseya Server-Standardwerten erstellt.

Neue Rechner-ID

Geben Sie einen eindeutigen Namen für die neue Rechner-ID ein, die Sie erstellen.

Gruppen-ID

Wählen Sie eine vorhandene Gruppen-ID für die neue Rechner-ID aus, die Sie erstellen. Der Standard ist `root.unnamed`. Gruppen-IDs werden von einem VSA-Benutzer über System > Org. / Gruppen / Abtlg.> **Verwalten** *(siehe 423)* erstellt.

Erstellen

Klicken Sie auf **Erstellen**, um die neue Rechner-ID für die ausgewählte Gruppen-ID zu erstellen.

Neue Konten einrichten/löschen, die in Gruppen-ID <Gruppen-ID>, Einstellungen kopieren von <Rechner-ID> erstellt wurden

Sie können für jede Gruppen-ID eine andere Standard-Rechner-ID angeben, von der die Einstellungen kopiert werden sollen.

1. Wählen Sie eine Rechner-ID aus, von der Einstellungen kopiert werden sollen, indem Sie auf das Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID klicken.
2. Wählen Sie eine Gruppen-ID aus der Dropdown-Liste mit den Gruppen-IDs aus.
3. Klicken Sie auf **Einrichten**, um sicherzustellen, dass die neue, für die ausgewählte Gruppen-ID erstellte Rechner-ID die Einstellungen von der ausgewählten Standard-Rechner-ID kopiert.
4. Klicken Sie auf den Link **Löschen**, um diese Zuweisung zu entfernen.

Konten einrichten/löschen, die in *nicht zugewiesenen* Gruppen-ID-Kopiereinstellungen von <Rechner-ID> erstellt wurden

Diese Option gibt die Standard-Rechner-ID an, von der Einstellungen kopiert werden sollen, falls keine Standard-Rechner-ID für eine Gruppen-ID eingestellt wurde. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

1. Wählen Sie eine Rechner-ID aus, von der Einstellungen kopiert werden sollen, indem Sie auf das Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID klicken. Anfangs ist dieser Wert auf *nicht zugewiesen* eingestellt.
2. Klicken Sie auf **Einrichten**, um sicherzustellen, dass neue, ohne Gruppen-Standard-Rechner-ID erstellte Rechner-IDs die Einstellung von der Standard-Rechner-ID des Benutzers mit Master-Rolle kopieren. Anfänglich ist dieser Wert auf *nicht zugewiesen* eingestellt.
3. Klicken Sie auf den Link **Löschen**, um diese Zuweisung zu entfernen.

Kontaktinformationen eingeben

Wenn Sie auf dieser Seite Kontaktinformationen für ein neues Rechner-ID-Konto eingeben und dieses neue Konto dann durch Klicken auf die Schaltfläche **Erstellen** anlegen, werden dieselben Kontaktinformationen auf die Seite Agent > **Profil bearbeiten** *(siehe 73)* übertragen. Die Kontaktinformationen umfassen Folgendes:

- **Kontakt-E-Mail** – Geben Sie die E-Mail-Adresse der Person ein, die den verwalteten Rechner benutzt.
- **Auto** – Aktivieren Sie **Auto**, um das Feld **Kontakt-E-Mail** automatisch mit einer E-Mail-Adresse im folgenden Format auszufüllen: `machineid@groupid.com`. Diese Funktion setzt voraus, dass Sie Rechner-IDs und Gruppen-IDs erstellen, die sich an die E-Mail-Adressen der Benutzer anpassen.
- **Kontaktname** – Geben Sie den Namen der Person ein, die den verwalteten Rechner benutzt.
- **Kontakt Telefon** – Geben Sie die Telefonnummer der Person ein, die den verwalteten Rechner benutzt.
- **E-Mail Administrator** – Geben Sie die E-Mail-Adresse der Person ein, die für den IT-Support für den verwalteten Rechner zuständig ist.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Einstellungen kopieren

Klicken Sie auf ein Optionsfeld neben einer im Seitenbereich aufgeführten Rechner-ID. Die Einstellungen der Rechner-ID werden von dieser Rechner-ID kopiert.

Agent-Installation herunterladen/per E-Mail versenden

Klicken Sie auf einen Link für eine Rechner-ID, um mithilfe des Assistenten **Agent herunterladen** ein Installationspaket für ein vorhandenes Rechner-ID-Konto zu erstellen und zu verteilen.

> **Hinweis:** Ein mit dieser Seite erstelltes Installationspaket gilt für spezifische Rechner-ID-Konten. Verwenden Sie **Agent verteilen** *(siehe 40)*, um Installationspakete für *mehrere* Rechner zu erstellen.

1. Wählen Sie das Betriebssystem aus, für das Sie das Installationspaket erstellen: `Windows`, `Macintosh` oder `Linux`.
2. Binden Sie optional die Anmeldedaten eines Benutzers an das Installationspaket. Füllen Sie das Formular mit den Administratoranmeldedaten aus, um die Benutzerrechte sicher an das Installationsformular zu binden.
   - Benutzer ohne Benutzerrechte können das Installationspaket erfolgreich installieren, ohne Administrator-Anmeldedaten eingeben zu müssen.
   - Wenn die Administrator-Anmeldedaten leer gelassen werden und der Benutzer keine Rechte zum Installieren von Software hat, wird er während der Installation vom Installationspaket zur Eingabe von Administrator-Anmeldedaten aufgefordert.
3. Wählen Sie die Verteilungsmethode aus.
   - **Herunterladen** – Laden Sie das Installationspaket sofort auf den gegenwärtig von Ihnen benutzten Rechner herunter. Der Name des Installationspakets lautet stets `KcsSetup`.
   - **E-Mail** – Senden Sie eine Textnachricht per E-Mail, die einen Link zum Herunterladen des Installationspakets enthält.

Typ

Dies ist der Typ des auf dem verwalteten Rechner verwendeten Betriebssystems:

- Fenster
- Macintosh
- Linux

Erstes Check-in

Listet die Uhrzeit auf, zu der jeder Agent sich zum ersten Mal am Kaseya Server angemeldet hat.

Löschen

Agent > Agents installieren > Löschen

Auf der Seite **Löschen** können drei verschiedene Kombinationen von *Rechner-ID-Konten* und *Agents* gelöscht werden.

Rechner-IDs vs. Agents

Bei der Erläuterung von Agents ist es nützlich, zwischen der **Rechner-ID/Gruppen-ID/Organisations-ID** *(siehe 626)* und dem **Agent** *(siehe 611)* zu unterscheiden. Die Rechner-ID/Gruppen-ID/Organisations-ID ist der **Kontoname** für einen verwalteten Rechner in der VSA-Datenbank. Der Agent ist die Clientsoftware, die auf dem verwalteten Rechner installiert ist. Zwischen dem Agent auf einem verwalteten Rechner und

seinem Kontonamen auf dem VSA besteht eine Eins-zu-Eins-Beziehung. Die Agent-Aktionen auf dem verwalteten Rechner werden von den Aufgaben geleitet, die einer Rechner-ID von VSA-Benutzern zugewiesen wurden.

Agent-Lizenzzahlen

Die folgenden Ereignisse wirken sich auf Agent-Lizenzzahlen aus:

- Eine "nicht verwendete" Agent-Lizenz wird in "verwendet" geändert, wenn ein Rechner-ID-Konto erstellt und der Agent installiert wird.
- Falls der Agent, aber nicht das Konto, gelöscht wird, wird die Agent-Lizenz dennoch als "verwendet" betrachtet.
- Wenn das Konto gelöscht wird (ungeachtet dessen, was mit dem Agent geschieht), erhält die Agent-Lizenz wieder den Status "nicht verwendet".
- Falls ein Konto erstellt wird, der Agent jedoch noch nicht zum ersten Mal installiert ist, wird das Konto als **Rechner-ID-Vorlage** *(siehe 627)* bezeichnet. Rechner-ID-Kontovorlagen werden erst als "verwendet" gezählt, wenn Sie den Agent installieren.

Löschen von Agents mit Tickets

Durch Löschen eines Rechnerkontos werden alle **Service Desk**-Tickets oder **Ticketing**-Tickets der Rechnergruppe oder Organisation, zu der das Rechnerkonto gehört hat, erneut zugeordnet.

Verfahren

1. Wählen Sie im Seitenbereich eine oder mehrere Rechner-IDs aus.
2. Klicken Sie auf eins der folgenden Optionsfelder:
   - **Agents erst bei der nächsten Anmeldung deinstallieren** – Deinstallieren Sie den Agent vom Rechner **und** entfernen Sie das Rechner-ID-Konto vom Kaseya Server. Das Konto wird erst bei der nächsten erfolgreichen Anmeldung des Agents gelöscht.
   - **Konto jetzt löschen, ohne den Agent zu deinstallieren** – Der Agent bleibt installiert **und** das Rechner-ID-Konto wird vom Kaseya Server entfernt.
   - **Agent deinstallieren und Konto beibehalten** – Deinstallieren Sie den Agent vom Rechner, **ohne** das Rechner-ID-Konto vom Kaseya Server zu entfernen.
3. Klicken Sie auf die Schaltfläche **Konten löschen**.

Hinweis: Durch die Deinstallation eines Agents wird K-VNC oder der KBU-Client, KES-Client oder KDPM-Client nicht entfernt. Vor dem Löschen des Agents verwenden Sie Fernsteuerung > **Fernsteuerung deinstallieren** *(siehe 381)*, um K-VNC auf den verwalteten Rechnern zu deinstallieren. Deinstallieren Sie ebenfalls alle Clients des Zusatzmoduls.

Wählen Sie alte Konten aus, die seit<Datum> nicht mehr angemeldet waren.

Klicken Sie auf den Hyperlink **Alte auswählen**, um alle Rechner-IDs im Seitenbereich zu markieren, die seit dem angegebenen Datum nicht mehr angemeldet waren. Dies stellt eine einfache Methode zum Identifizieren und Entfernen veralteter Rechner-IDs dar.

Datenbank bereinigen

Das Entfernen eines Rechner-Kontos über diese Seite **Löschen** markiert das Rechnerkonto für den Löschvorgang. Der tatsächliche Löschvorgang findet normalerweise außerhalb der Arbeitsstunden statt, um die Ressourcen während des Arbeitstages zu schonen. In einigen Fällen ist es nützlich, Rechnerkonten sofort zu bereinigen. Beispielsweise könnte der Kaseya Server die Agent-Lizenzzahl überschreiten. Klicken Sie auf **Datenbank bereinigen**, um Rechnerkonten sofort zu löschen, die bereits für den Löschvorgang markiert wurden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem

Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Letzter Check-in

Zeigt die Uhrzeit an, zu der der Rechner-Agent zum letzten Mal am Kaseya Server angemeldet waren. Bei Agents, die länger nicht angemeldet waren, werden diese Informationen als roter Text angezeigt.

Umbenennen

Agent > Agents installieren > Umbenennen

Auf der Seite **Umbenennen** werden vorhandene Rechner-ID-Konten umbenannt. Sie können die Rechner-ID ändern und/oder einer anderen Gruppen-ID zuweisen.

Agents werden durch eine eindeutige GUID-Nummer identifiziert. Durch ein Umbenennen des Agents wird nur der Anzeigename des Agenta geändert, und zwar sowohl auf dem Kaseya Server als auch in der Option **Konto festlegen...** im Agent-Menü des verwalteten Rechners.

> **Hinweis:** Informationen über das Zuweisen mehrerer Rechner zu einer anderen Gruppen-ID finden Sie unter Agent > **Gruppe ändern** *(siehe 62)*.

Verfahren

1. Wählen Sie im Seitenbereich eine Rechner-ID aus.
2. Klicken Sie auf eins der folgenden Optionsfelder:
   - **Konto umbenennen** – Wählen Sie diese Option aus, um ein ausgewähltes Rechner-ID-Konto umzubenennen.
   - **Offline Konto zusammenführen <Offline Rechner-ID> in <Rechner-ID auswählen> <Offline Rechner-ID>nach Zusammenführung** löschen – Verwenden Sie die Zusammenführung, um Protokolldaten von zwei verschiedenen Konten auf demselben Rechner zu kombinieren. Dies könnte notwendig sein, wenn ein Agent deinstalliert und dann unter einem anderen Kontonamen neu installiert wurde. Bei einer Zusammenführung werden die Konten wie folgt kombiniert:
     - ✓ Protokolldaten von beiden Konten werden kombiniert.
     - ✓ Daten des **Basis-Audits** *(siehe 615)* vom alten Offline Konto ersetzen alle Ausgangsdaten

im ausgewählten Konto.

- ✓ Meldungseinstellungen vom ausgewählten Konto bleiben erhalten.
- ✓ Anstehende Agent-Verfahren vom ausgewählten Konto bleiben erhalten. Anstehende Agent-Verfahren vom alten Offline-Konto werden verworfen.
- ✓ Das alte Konto wird nach der Zusammenführung gelöscht.

Hinweis: Da der Rechner nur auf einem einzigen Konto aktiv sein kann, werden nur Offline-Konten zur Zusammenführung in der Dropdown-Liste angezeigt.

3. Geben Sie optional einen **Neuen Namen** für das Rechner-ID-Konto ein.
4. Wählen Sie optional eine andere **Gruppen-ID** für das Rechner-ID-Konto aus.
5. Klicken Sie auf die Schaltfläche **Umbenennen**.

Umbenennen

Klicken Sie auf **Umbenennen**, um den Namen eines ausgewählten Rechner-ID-Kontos mithilfe der früher ausgewählten Optionen zu ändern.

Neuer Name

Geben Sie den **Neuen Namen** für die ausgewählte Rechner-ID ein.

Gruppen-ID

Wählen Sie die **Gruppen-ID** aus, die dem ausgewählten Rechner-ID-Konto zugewiesen werden soll. Bei Wahl des Standardwerts bleibt die Gruppen-ID unverändert.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen. Klicken Sie auf das Optionsfeld links von dem Rechnerkonto, das Sie umbenennen möchten.

Neuer Name beim nächsten Check-in

Listet den neuen Namen auf, auf den das Konto bei der nächsten Anmeldung des Agents umbenannt wird. Hier werden nur anstehende Umbenennungen angezeigt.

Gruppe ändern

Agent > Agents installieren > Gruppe ändern

Auf der Seite **Gruppe ändern** werden mehrere Rechner-IDs zu verschiedenen Gruppen-IDs zugewiesen. Rechner, die gegenwärtig offline sind, werden bei ihrem nächsten Check-in zugewiesen.

Rechner-ID in eine andere Gruppe verschieben

1. Wählen Sie im Seitenbereich eine oder mehrere Rechner-IDs aus.
2. Wählen Sie eine Gruppen-ID aus dem Dropdown-Menü **Neue Gruppen-ID auswählen** aus.
3. Klicken Sie auf die Schaltfläche **Verschieben**.

Verschieben

Weist ausgewählte Rechner-IDs zur ausgewählten Gruppen-ID zu.

Neue Gruppen-ID auswählen

Geben Sie die neue Gruppen-ID an, die jeder ausgewählten Rechner-ID zugewiesen werden soll.

> **Hinweis:** Erstellen Sie über System > Benutzersicherheit > **Scopes** *(siehe 419)* eine neue Rechnergruppen-ID oder Untergruppen-ID.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Einstellungen kopieren

Agent > Agent konfigurieren > Einstellungen kopieren

Auf der Seite **Einstellungen kopieren** können Sie ausgewählte Einstellungen von einer einzigen Quellrechner-ID auf mehrere Rechner-IDs kopieren. Sie können Einstellungen jeweils *von nur einer Quell*rechner-ID oder -Vorlage kopieren. Aber Sie können verschiedene Einstellungstypen von verschiedenen Quellrechner-IDs oder -Vorlagen in Folge kopieren.

Einstellungen und Vorlagen kopieren

Rechner-ID-Vorlagen *(siehe 627)* werden anfänglich dazu verwendet, um ein Agent-Installationspaket zu erstellen. Dabei wird die Vorlage als Quelle verwendet, um Einstellungen zu kopieren. Aber selbst nach der Installation der Agents auf verwalteten Rechnern müssen Sie die Einstellungen auf vorhandenen Rechner-ID-Konten aktualisieren, da sich die Anforderungen Ihrer Kunden ändern und Sie sich immer besser mit dem VSA auskennen. Verwenden Sie in diesem Fall Agent > **Einstellungen kopieren**, um diese Änderungen auf alle Rechner-IDs zu kopieren, für die Sie Zugriffsberechtigungen haben. Achten Sie darauf, `Do Not Copy` für jede Einstellung auszuwählen, die Sie nicht überschreiben möchten. Verwenden Sie `Add`, um Einstellungen zu kopieren, ohne vorhandene Einstellungen zu entfernen. Kaseya empfiehlt, zuerst die Änderungen an einer ausgewählten Vorlage vorzunehmen und diese Vorlage dann als Quellrechner-ID zum Kopieren zu verwenden. Auf diese Weise wird sichergestellt, dass Ihre Rechner-ID-Vorlagen die "Master-Repositories" aller Ihrer Agent-Einstellungen bleiben und als Quelle für die Agent-Installationspakete und vorhandenen Rechner-ID-Konten dienen können.

Kopie

Klicken Sie auf **Kopieren**, um einen Quellrechner auszuwählen. Nach Auswahl des Quellrechners werden die Einstellungstypen, die Sie kopieren können, in einem zweiten Fenster angezeigt.

Indem Sie nur bestimmte Typen von Einstellungen zum Kopieren auswählen, können Sie verhindern, dass kundenspezifische Einstellungen überschrieben werden, die Sie beibehalten möchten. Dazu zählt z. B. die `Patch File Source`, die für jeden Kunden unterschiedlich ist.

Wählen Sie die Option `Add` aus, um Einstellungen zu Zielrechnern hinzuzufügen, ohne vorhandene Einstellungen zu ersetzen.

Es können folgende Typen von Agent-Einstellungen kopiert werden:

- Anmeldedaten
- Agent-Menü
- Check-in-Kontrolle
- Arbeitsverzeichnis
- Protokolle
- Rechnerprofil – Verweist auf Einstellungen in Inventarisierung > **Profil bearbeiten** *(siehe 73)*.
- Sammlungen ansehen
- Portalzugriff
- Remote-Control-Richtlinie
- Patch-Einstellungen
- Patchdateiquelle
- Zugehörigkeit zu Patch-Richtlinien
- Feste Meldungen – Diese Meldungstypen werden alle auf der Seite Monitor > **Meldungen** *(siehe 284)* angezeigt, mit Ausnahme von `Event Log`-Meldungen und `System`-Meldungen.
- Ereignisprotokoll-Meldungen
- Monitor-Sets
- Dateien verteilen
- Schutz
- Geplante Skripte

Wählen Sie die Rechner-ID aus

Klicken Sie auf den Link **Rechner-ID auswählen**, um anzugeben, von welcher Rechner-ID die Einstellungen kopiert werden sollen.

Verteilen Sie die geplanten Skripte auf unterschiedliche Zeiten, wenn Sie sie auf mehrere Rechner kopieren

Sie können die Last auf das Netzwerk verteilen, indem Sie diese Aufgabe staffeln. Wenn Sie diesen

Parameter auf 5 Minuten einstellen, wird der Scan auf jeder Rechner-ID um 5 Minuten versetzt. Beispiel: Rechner 1 läuft um 10:00, Rechner 2 läuft um 10:05, Rechner 3 läuft um 10:10.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Status

Zeigt den Rechnernamen, von dem die Einstellungen kopiert wurden und die Uhrzeit des Kopiervorgangs.

Import/Export

Agent > Agent konfigurieren > Import/Export

Auf der Seite **Import/Export** können Einstellungen für Rechner-ID-Konten als XML-Dateien importiert und exportiert werden, einschließlich geplanter Agent-Verfahren, zugewiesener Monitor-Sets und Ereignissätze. Protokolldaten sind nicht im Import oder Export eingeschlossen. Mit **Import/Export** können Sie Einstellungen für Rechner-ID-Konten, darunter **Rechner-ID-Vorlagen** *(siehe 627)*, von einem Kaseya Server zum nächsten migrieren.

- Stellen Sie beim Importieren einer XML-Datei sicher, dass die Verschlüsselung der Datei ISO-8859-1 lautet.
- Eine Liste der mit einem Rechner-ID-Konto verknüpften Einstellungstypen finden Sie unter **Einstellungen kopieren** *(siehe 62)*.
- Die neuesten Anweisungen zur Migration eines vorhandenen Kaseya Server auf einen neuen Rechner finden Sie im Abschnitt *Verschieben des Kaseya Server* in den aktuellen **Kaseya Server-Installationsanweisungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/Install/index.asp#home.htm)*.
- Beispielvorlagen für bestimmte Rechnertypen können Sie von unserer Website aus dem Kaseya Forum **Kaseya Connections** unter **http://community.kaseya.com** *(http://community.kaseya.com)* kopieren.

So exportieren Sie Rechner-ID-Einstellungen:

1. Klicken Sie auf den Link **Rechner auswählen**. Es wird ein Dialogfeld zur Auswahl des Rechners angezeigt.

2. Filtern Sie optional die Anzeige der aufgelisteten Rechner-IDs unter Verwendung des **Rechner-ID/Gruppen-ID-Filters** *(siehe 626)*.
3. Klicken Sie auf einen Rechner-ID-Link für den Export. Die ausgewählte Rechner-ID wird nun auf der Seite **Import/Export** angezeigt.
4. Klicken Sie auf **Export**. Die Seite zeigt einen XML-Auszug der exportierten Agent-Einstellungen an.
5. Exportieren Sie die XML-Anweisung wie folgt:
   - Kopieren Sie den XML-Text in die Zwischenablage.
   - Klicken Sie mit der rechten Maustaste auf den Link **Herunterladen** und wählen Sie die Option **Ziel speichern unter**, um den XML-Text als XML-Datei auf Ihrem lokalen Computer zu speichern.

So importieren Sie Rechner-ID-Einstellungen:

1. Stellen Sie beim Importieren einer XML-Datei sicher, dass die Verschlüsselung der Datei ISO-8859-1 lautet.
2. Klicken Sie auf **Blättern**, um eine XML-Datei auszuwählen, die die Einstellungen eines Rechner-ID-Kontos darstellt. Normalerweise werden diese XML-Dateien durch den Export von einem anderen Kaseya Server erstellt.
3. Klicken Sie auf **Import**. Es wird ein Satz zusätzlicher Optionen angezeigt.
4. Akzeptieren Sie den Namen der Rechner-ID oder geben Sie einen an. Wenn dieser Name noch nicht auf dem Kaseya Server vorhanden ist, wird ein neuer Name erstellt.
5. Akzeptieren Sie oder wählen Sie eine andere Gruppen-ID aus.
6. Aktivieren Sie optional das Kontrollkästchen neben **Bestehende Daten ersetzen, falls diese Rechner-ID bereits existiert**.
7. Ändern Sie optional die E-Mail-Benachrichtigungsadresse für alle Meldungen, die für dieses Rechner-ID-Konto definiert sind.
8. Klicken Sie auf **Fertig stellen**, um den Import abzuschließen.

Aussetzen

Agent > Agent konfigurieren > Aussetzen

Auf der Seite **Aussetzen** werden alle Agent-Operationen, z. B. Agent-Verfahren, Monitoring und Patching ausgesetzt, ohne die Einstellungen des Agents zu ändern. Wenn eine Aktion ausgesetzt wird, erscheint neben der Rechner-ID wird das Symbol Aussetzen. Wenn ein Rechner-ID-Konto ausgesetzt ist, wird auf dem verwalteten Rechner ein graues Agent-Symbol in der **Systemablage** *(on seite 631)*angezeigt.

Mit der Option **Rechner zeigen, die ausgesetzt/nicht ausgesetzt sind** in **Ansichtdefinitionen** *(siehe 27)* können Sie die Anzeige der Rechner-IDs auf jeder Agent-Seite filtern.

Aussetzen

Klicken Sie auf **Aussetzen**, um Agent-Operationen auf ausgewählten Rechner-IDs auszusetzen.

Fortsetzen

Klicken Sie auf **Fortsetzen**, um Agent-Operationen auf ausgewählten Rechner-IDs fortzusetzen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Ausgesetzt

Zeigt `Suspended` an, wenn die Rechner-ID ausgesetzt ist.

Agent-Menü

Agent > Agent konfigurieren > Agent-Menü

Auf der Seite **Agent-Menü** werden die Optionen festgelegt, die im Agent-Menü des Rechners eines Benutzers angezeigt werden. Der Benutzer zeigt das Agent-Menü an, indem er mit der rechten Maustaste auf das Agent-Symbol in der **Systemablage** *(on seite 631)*des verwalteten Rechners klickt. Über diese Seite kann außerdem *verhindert werden*, dass das Agent-Symbol auf dem Rechner des Benutzers angezeigt wird. Mithilfe dieser Seite vorgenommene Änderungen werden beim nächsten Agent-Check-in wirksam und bis dahin als roter Text angezeigt.

> **Hinweis:** Eine allgemeine Erläuterung der Anzeige von Agent-Symbolen auf dem Rechner des Benutzers finden Sie unter **Agent-Symbole** *(siehe 24)*.

Agent-Symbol auf dem Rechner des Benutzers ausblenden

So blenden Sie das Agent-Symbol vollkommen aus:

1. Wählen Sie eine oder mehrere Rechner-IDs aus.
2. Deaktivieren Sie das Kontrollkästchen **Agent-Symbol aktivieren**.
3. Klicken Sie auf **Aktualisieren**.

Alle anderen Kontrollkästchen-Einstellungen werden abgeblendet angezeigt. Dies bedeutet, dass alle Optionen des Agent-Menüs deaktiviert wurden.

Benutzer daran hindern, den Agent-Dienst auf dem Rechner zu beenden

Falls die Option **Beenden** auf dem verwalteten Rechner eines Benutzers aktiviert ist, kann er den Agent-Dienst auf dem Rechner durch Auswahl dieser Option beenden. Wenn der Agent-Dienst angehalten wird, wird der verwaltete Rechner für VSA-Benutzer als offline angezeigt und kann keine Befehle mehr vom Kaseya Server empfangen.

So entfernen Sie die Option **Beenden** aus Agent-Menüs auf verwalteten Rechnern:

1. Wählen Sie eine oder mehrere Rechner-IDs aus.
2. Deaktivieren Sie das Kontrollkästchen **Beenden**.
3. Klicken Sie auf **Aktualisieren**.

Kontrollkästchen

- **Agent-Symbol aktivieren** – Aktivieren Sie dieses Kontrollkästchen, um das Agent-Symbol in der Systemablage des verwalteten Rechners anzuzeigen. Deaktivieren Sie dieses Kontrollkästchen, um das Agent-Symbol auszublenden und die Verwendung von Agent-Menü-Optionen zu verhindern.
- **Über<Agent>** – Aktivieren Sie dies, damit der Rechnerbenutzer auf diese Option klicken kann, um das Feld Info für den installierten Agent anzuzeigen. Die Standard-Optionsbezeichnung `Agent` kann angepasst werden.
- **<Administrator kontaktieren...>** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um entweder die Seite **Portal-Zugang** *(siehe 625)* oder eine andere URL anzuzeigen. Die Standard-Optionsbezeichnung `Contact Administrator...` kann angepasst werden.
- **<URL Ihres Unternehmens...>** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um die im entsprechenden URL-Feld angegebene URL anzuzeigen.
- **Fernsteuerung deaktivieren** – Aktvieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um die Fernsteuerung auf dem verwalteten Rechner des Benutzers zu *deaktivieren*.
- **Konto festlegen...** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um seine Rechner-ID.Gruppen-ID.Organisations-ID anzuzeigen und die Kaseya Server-Adresse für die Agent-Anmeldung zu ändern. Die von Ihnen eingegebene, neue IP-Adrresse muss auf einen funktionierenden VSA verweisen. Ansonsten tritt die Änderung der IP-Adresse nicht in Kraft.
- **Aktualisieren** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer eine sofortige **vollständige Anmeldung** *(siehe 616)* einleiten kann.
- **Beenden** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer den Agent-Dienst auf dem verwalteten Rechner beenden kann.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um Einstellungen des Agent-Menüs auf ausgewählte Rechner-IDs anzuwenden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ACObSRx

Diese Spalte fasst die aktivierten Optionen des Agent-Menüs für eine Rechner-ID zusammen. **ÜBOtKAe** steht für die Tastaturkürzel, mit denen auf jede Option im Agent-Menü zugegriffen werden kann.

Ein Buchstabe deutet darauf hin, dass diese Option im Agent-Menü angezeigt wird. Ein "-" weist darauf hin, dass diese Menüoption nicht im Agent-Menü angezeigt wird.

Ü = **Ü**ber Agent

B = **B**enutzer kontaktieren

O = Startet die im URL-Feld angegebene URL. Der Agent zeigt den Text aus dem Feld links vom URL-Feld an.

t = Fernsteuerung deak**t**ivieren

K = **K**onto einrichten...

A = **A**ktualisieren

e = Be**e**nden

Über den Titel

Der Text, der der Bezeichnung für die Option **Info** im Agent-Menü angehängt wurde. Wenn beispielsweise der Info-Titel `Agent` lautet, wird die Bezeichnung der Option **Über** als `About Agent` angezeigt.

Kontakttitel

Der Text, der im Agent-Menü als Kontakt für einen VSA-Benutzer angezeigt wird

Benutzerdefinierter Titel

Der Text, der im Agent-Menü als Kontakt für eine benutzerdefinierte URL angezeigt wird.

Kontakt-URL

Die URL, die angezeigt werden soll, wenn die Option `Contact Administrator...` vom Rechnerbenutzer ausgewählt wird. Die Standard-URL ist die Seite **Portalzugriff** *(siehe 75)*. Es kann eine andere URL eingegeben werden.

Benutzerdefinierte URL

Die URL, die angezeigt wird, wenn der Benutzer diese Option im Agent-Menü auswählt.

Check-in-Kontrolle

Agent > Agent konfigurieren > Check-in-Kontrolle

Auf der Seite **Check-in-Kontrolle** wird angegeben, wann und wo jeder Agent sich an einem Kaseya Server anmelden sollte. Sie können die primären und sekundären Kaseya Server-Namen/IP-Adressen für die Agent-Anmeldung, die von einem Agent zur Ausführung einer Aufgabe verbrauchte Bandbreite und den Anmeldungszeitraum festlegen.

- Der Agent meldet sich nur beim primären und nicht beim sekundären Server an, es sei denn, der primäre Server geht offline.
- Die primären und sekundären Kaseya Server-Werte und minimalen und maximalen Anmeldeperioden unterliegen den Richtlinien, die über System > **Anmelderichtlinie** *(siehe 405)*

eingerichtet wurden. Dies hindert Benutzer daran, Einstellungen auszuwählen, die den Servern, auf denen der Kaseya Server-Dienst ausgeführt wird, eine unnötige Last auferlegen.

- Mithilfe dieser Seite vorgenommene Änderungen werden beim nächsten Agent-Check-in wirksam und bis dahin als roter Text angezeigt.
- Daten zur **Check-in-Kontrolle** können auch über die Registerkarte **Agent-Einstellungen** der Seiten **Live Connect** *(siehe 60)* und **Rechnerübersicht** *(siehe 151)* gepflegt werden.

Beschränkungen des sekundären Servers

Fernsteuerungsfunktionen werden über die primäre Kaseya Server-Adresse übermittelt. Wenn sich ein Agent bei der sekundären Kaseya Server-Adresse anmeldet, stellen Fernsteuerungssitzungen keine Verbindung her, da sie an die falsche VSA-Übermittlungs-Serveradresse geleitet werden. Alle anderen Funktionen werden unterstützt und vom sekundären Kaseya Server auf gleiche Weise wie die primäre Kaseya Server-Adresse geplant.

Agents zwischen Kaseya Server migrieren

Eventuell entscheiden Sie sich aus Gründen der Leistung oder Logistik, verwaltete Rechner auf einen neuen Kaseya Server zu migrieren. Dies kann jederzeit ausgeführt werden und es kommt nicht darauf an, ob die Agents gegenwärtig angemeldet sind.

1. Stellen Sie auf dem **Original**-Kaseya Server die **primäre** Kaseya Server-Einstellung so ein, dass sie auf die **neue** Kaseya Server-Adresse verweist.
2. Stellen Sie auf dem **Original**-Kaseya Server die **sekundäre** Kaseya Server-Einstellung so ein, dass sie auf die **Original**-Kaseya Server-Adresse verweist.
3. Stellen Sie auf dem **neuen** Kaseya Server sowohl die **primäre** als auch die **sekundäre** Kaseya Server-Einstellung so ein, dass sie auf den **neuen** Kaseya Server verweist.
4. Warten Sie darauf, dass sich alle Agents erfolgreich am **neuen** Kaseya Server anmelden. Zu diesem Zeitpunkt kann der **Original**-Kaseya Server offline gesetzt werden.

> **Hinweis:** Die neuesten Anweisungen zur Migration eines vorhandenen Kaseya Server auf einen neuen Rechner finden Sie im Abschnitt *Verschieben des Kaseya Server* in den aktuellen **Kaseya Server-Installationsanweisungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/Install/index.asp#home.htm)*.

Port ändern, der von Agents für die Anmeldung am Kaseya Server verwendet wird

1. Stellen Sie den **primären** Port auf den **neuen** Port ein.
2. Stellen Sie den **sekundären** Port auf den **alten** Port ein.
3. Warten Sie darauf, dass die neuen Einstellungen für alle Agents wirksam werden.
4. Zeigen Sie die Seite System > **Konfigurieren** *(siehe 429)* an. Geben Sie die neue Portnummer in das Bearbeitungsfeld **Serverport angeben, über den die Agents einchecken** ein und klicken Sie auf die Schaltfläche **Port ändern**.

> **Hinweis:** Falls Agents vor dem Wechsel des Kaseya Server noch nicht zum neuen Port migriert sind, müssen Sie den Port manuell auf den verwalteten Rechnern ändern. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol in der Systemablage, um das Agent-Menü auf dem verwalteten Rechner anzuzeigen, und wählen Sie die Option **Konto festlegen...** aus. Geben Sie die Serveradresse und den Serverport ein. Zum Beispiel: `192.168.1.7:1234`.

Primärer KServer

Geben Sie die IP-Adresse oder den vollständig qualifizierten **Hostnamen** *(see "Hostname" on seite 619)* des primären Kaseya Server der Rechner-ID ein. Diese Einstellung wird in der Spalte **Primärer Kaseya Server** angezeigt.

Kaseya-Agents leiten sämtliche Kommunikationen mit dem Kaseya Server ein. Aus diesem Grund

müssen sie immer in der Lage sein, den Domänennamen oder die IP-Adresse (Internet Protocol) zu erreichen, der/die dem Kaseya Server zugewiesen wurde. Wählen Sie eine IP-Adresse oder einen Domänennamen, der von allen gewünschten Netzwerken (sowohl im lokalen LAN und im Internet) aus aufgelöst werden kann.

Best Practices: Obwohl eine öffentliche IP-Adresse verwendet werden kann, empfiehlt Kaseya die Verwendung eines **Domain Name Server (DNS)**-Namens für Kaseya Server. Dies wird als Vorsichtsmaßnahme empfohlen, falls die IP-Adresse geändert werden muss. Es ist einfacher, den DNS-Eintrag zu ändern, als verwaiste Agents umzuleiten.

Primärer Port

Geben Sie die Portnummer des primären Kaseya Server oder eines virtuellen Systemservers ein. Diese Einstellung wird in der Spalte **Primärer KServer** angezeigt.

Warnung: Verwenden Sie KEINEN *Rechnernamen* für Ihren Server. Der Agent verwendet standardmäß WinSock-Aufrufe, um einen vollständig qualifizierten **Hostnamen** *(see "Hostname" on seite 619)* in eine IP-Adresse aufzulösen, die für alle Agent-Verbindungen verwendet wird. Der Rechnername wird von NETBIOS in eine IP-Adresse aufgelöst. Dies ist eventuell nicht auf jedem Rechner aktiviert. NETBIOS ist eine optionale letzte Methode, die Windows zum Auflösen eines Namens einsetzt. Daher werden nur vollständig qualifizierte Namen oder IP-Adressen unterstützt.

Sekundärer KServer

Geben Sie die IP-Adresse oder den vollständig qualifizierten Hostnamen des sekundären Kaseya Server der Rechner-ID ein. Diese Einstellung wird in der Spalte **Sekundärer KServer** angezeigt. Der Agent meldet sich nur beim primären und nicht beim sekundären Server an, es sei denn, der primäre Server geht offline.

Sekundärer Port

Geben Sie die Portnummer des sekundären Kaseya Server oder eines virtuellen Systemservers ein. Diese Einstellung wird in der Spalte **Sekundärer KServer** angezeigt.

Check-in-Periode

Geben Sie das Zeitintervall ein, wie lange ein Agent warten soll, bevor er eine **Schnellanmeldung** *(siehe 616)* mit dem Kaseya Server ausführt. Eine Anmeldung nimmt eine Prüfung im Hinblick auf eine neue Aktualisierung des Rechner-ID-Kontos vor. Wenn eine neue Aktualisierung von einem VSA-Benutzer eingestellt wurde, beginnt der Agent mit der Aufgabe bei der nächsten Anmeldung. Diese Einstellung wird in der Spalte **Anmeldezeitraum** angezeigt. Die minimal und maximal zulässigen Check-in-Perioden werden über System > **Anmelderichtlinie** *(siehe 405)* eingerichtet.

Best Practices: Der Agent erhält eine ständige Verbindung mit dem Kaseya Server aufrecht. Daher wirken sich Schnellanmeldungszeiten nicht auf die Reaktionszeiten des Agents aus. Die Schnellanmeldungszeit legt die maximale Wartezeit fest, bevor eine ausgefallene Verbindung wiederhergestellt wird. Die Einrichtung der Schnellanmeldung der Rechner auf 30 Sekunden garantiert, dass sich jeder Agent innerhalb von 30 Sekunden von einer ausgefallenen Verbindung erholt. Dabei wird vorausgesetzt, dass die Verbindung erfolgreich ist.

An Kserver binden

Wenn as Kontrollkästchen aktiviert ist, ist der Agent an eine **eindeutige Kaseya Server-ID** gebunden. Gebundene Agents können erst dann einchecken, wenn die eindeutige Kaseya Server-ID, an die sie über "Agent > **Check-in-Kontrolle** *(siehe 68)*" gebunden wurden, der eindeutigen ID des Kaseya Server unter "System > **Konfigurieren** *(siehe 429)* > **ID ändern**" entspricht. Dadurch wird das Spoofing der

IP-Adresse durch Umleitung von Agent-Check-ins verhindert. Ein Schloss-symbol im Seitenbereich zeigt, dass der Agent gebunden ist. Um Agents zu *lösen*, wählen die Rechner-IDs aus, entfernen das Häkchen bei **An Kserver binden** und klicken auf **Aktualisieren**. Das Schloss-symbol wird die ausgewählten Rechner nicht mehr angezeigt.

Bandbreitendrosselung

Mit dieser Funktion beschränken Sie den Agent auf den Verbrauch einer Höchstmenge an Bandbreite im System. Standardmäßig teilt sich der Agent die Bandbreite mit allen anderen laufenden Anwendungen, sodass normalerweise keine Bandbreitendrosselung aktiviert werden muss. Deaktivieren Sie die Bandbreitendrosselung, indem Sie eine 0 eingeben.

Warnen, wenn mehrere Agents das gleiche Konto verwenden

Der Kaseya Server kann ermitteln, wenn mehr als ein Agent eine Verbindung mit dem Kaseya Server herstellt und dieselbe Rechner-ID.Gruppen-ID.Organisations-ID verwendet. Dieses Problem könnte durch das Installieren eines mit der Rechner-ID vorkonfigurierten Agent-Installationspakets auf mehr als einem Rechner verursacht werden. Markieren Sie dieses Kontrollkästchen, um jedes Mal, wenn Sie sich als Benutzer beim Kaseya Server anmelden, Benachrichtigungen über mehrere Agents zu erhalten, die das gleiche Konto verwenden.

Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist

Wenn Sie Rechner verwalten, die das gleiche LAN nutzen wie Ihr Kaseya Server, erhalten Sie möglicherweise diese Warnung. Standardgemäß verbinden sich alle Agents mit dem/der gleichen **externen Namen/IP-Adresse** *(siehe 429)* zurück zum Kaseya Server. TCP/IP-Meldungen dieser Agents werden über Ihr internes LAN an Ihren Router und anschließend zurück zum Kaseya Server geleitet. Einige Router leiten internen Verkehr mehr schlecht als recht durch sich selbst zurück. Markieren Sie dieses Kontrollkästchen, um eine Meldung zu erhalten, wenn der Kaseya Server einen Agent im selben LAN ermittelt, der über den Router verbunden ist.

> **Hinweis:** Agents im selben LAN wie der Kaseya Server sollten die gemeinsame interne IP-Adresse des Agents und des Kaseya Server angeben, die auf der Seite **Anmeldesteuerung** *(siehe 68)* festgelegt wurde.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um alle ausgewählten Rechner-IDs mit den vorher ausgewählten Optionen zu aktualisieren.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Arbeitsverzeichnis

Agent > Agent konfigurieren > Arbeitsverzeichnis

Auf der Seite **Arbeitsverzeichnis** wird ein Pfad zu einem Verzeichnis auf dem verwalteten Rechner eingestellt, das vom Agent zum Speichern der Arbeitsdateien verwendet wird.

Je nach der anliegenden Aufgabe verwendet der Agent mehrere zusätzliche Dateien. Der Server überträgt diese Dateien in ein Arbeitsverzeichnis, das vom Agent auf dem verwalteten Rechner verwendet wird. Bei ausgewählten Rechner-IDs können Sie das Standard-Arbeitsverzeichnis von `C:\kworking` in einen anderen Speicherort ändern.

> **Warnung: Löschen Sie keine Dateien und Ordner im Arbeitsverzeichnis.** Der Agent verwendet die im Arbeitsverzeichnis gespeicherten Daten, um verschiedene Aufgaben auszuführen.

Sie können dieses Verzeichnis in Sicherheitsprogrammen (z. B. Virenprüfprogramme) bestätigen, um zu verhindern, dass Vorgänge wie etwa die Fernsteuerung blockiert werden.

> **Hinweis:** Ein Arbeitsverzeichnis kann auch über die Registerkarte **Agent-Einstellungen** der Seiten **Live-Connect** *(siehe 393)* und **Rechnerübersicht** *(siehe 151)* gepflegt werden. Mithilfe des Befehls **getVariable()** in Agent-Verfahren kann in das Arbeitsverzeichnis geschrieben werden.

Übernehmen

Klicken Sie auf **Einrichten**, damit ausgewählte Rechner-IDs das vorher eingegebene Arbeitsverzeichnis verwenden.

Stellen Sie einen Pfad zum Verzeichnis her, das vom Agent für die Speicherung der Arbeitsdateien verwendet wird

Geben Sie den Pfad des Arbeitsverzeichnisses ein, das vom Agent auf dem verwalteten Rechner verwendet wird.

Als Systemstandard einstellen

Klicken Sie auf **Als Systemstandard einstellen**, um einen systemweiten Standard für das Agent-Arbeitsverzeichnis festzulegen. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten

nicht aktiv

- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Pfad für Arbeitsverzeichnis

Der Pfad des Arbeitsverzeichnisses, das dieser Rechner-ID zugewiesen wurde. Auf einem Apple OS X-System muss dem Pfad ein Schrägstrich vorangestellt werden, wenn er eine Leerstelle enthält. Zum Beispiel: `/tmp/name\ with\ three\ spaces`

Profil bearbeiten

Agent > Agent konfigurieren > Profil bearbeiten

Auf der Seite **Profil bearbeiten** werden Kontaktinformationen, die Sprache des Agent-Menüs auf dem Rechner des Benutzers und Anmerkungen zu jedem Rechner-ID-/Gruppen-ID-Konto gepflegt. Die Profilinformationen können an drei anderen Stellen gepflegt werden:

- Die Kontaktinformationen auf der Seite **Profil bearbeiten** können automatisch ausgefüllt werden, wenn über die Seite Agent > **Erstellen** *(siehe 55)* ein neues Konto erstellt wird.
- Sowohl VSA-Benutzer als auch Rechnerbenutzer können Kontaktinformationen über die Registerkarte Startseite > **Profil ändern** im Fenster **Live-Connect** *(siehe 393)* oder **Portalzugriff** *(siehe 75)* ändern.
- Nur VSA-Benutzer können Anmerkungen und Kontaktinformationen auch über die Registerkarte **Agent-Einstellungen** der Seiten **Live-Connect** *(siehe 393)* und **Rechnerübersicht** *(siehe 151)* pflegen.

So ändern Sie die Einstellungen der Benutzerkonten:

1. Wählen Sie im Seitenbereich eine Rechner-ID aus.
2. Geben Sie die Informationen für **Anmerkungen**, **Admin-E-Mail**, **Kontaktname**, **Kontakt-E-Mail** und **Kontakt Telefon** ein.
3. Klicken Sie auf **Aktualisieren**.

Spezielle Anweisungen

Geben Sie Anmerkungen zu einem Rechner-ID-Konto ein. Hilfreiche Daten sind zum Beispiel Standort des Rechners, Rechnertyp, Firma oder sonstige Erkennungsdaten zum verwalteten Rechner. Diese speziellen Anweisungen werden angezeigt, wenn Sie den Cursor über ein Agent-Statussymbol mit einem Zeichen bewegen. Im Fenster **Schnellansicht** *(siehe 17)* wird der Text mit den **speziellen Anweisungen** unten im Fenster angezeigt.

Symbol-Abzeichen

Fügen Sie *Zeichen* zur unteren rechten Ecke des Agentstatussymbols hinzu, wie . Diese Zeichen werden überall angezeigt, wo das Agent-Symbol in der Benutzeroberfläche erscheint. Sie können beispielsweise einen Rechner mit einem -Zeichen versehen, um anzugeben, dass der Kunde einen Telefonanruf bekommen muss, bevor jemand an diesem Rechner arbeitet. Sie können einen Server auch mit einem -Zeichen markieren, damit dieser erst nach Betriebsschluss verwendet wird.

Wählen Sie auf der Seite Agent > **Profil bearbeiten** *(siehe 73)* mindestens einen Rechner aus. Klicken Sie

anschließend auf den Link **Symbol-Abzeichen** oben auf der Seite und wählen Sie eines der verfügbaren Zeichen aus. Sie können eine Textnachricht mit **speziellen Anweisungen** für jedes Zeichen definieren. Klicken Sie auf die Schaltfläche **Aktualisieren**, um das Zeichen ausgewählten Rechnern zuzuweisen.

Wenn Sie den Cursor über ein Agent-Statussymbol mit einem Zeichen bewegen, wird das Fenster **Schnellansicht** *(siehe 17)* im Text mit den **speziellen Anweisungen** unten im Fenster angezeigt.

Tickets automatisch zuweisen

Weisen Sie automatisch ein Ticket zu dieser Rechner-ID zu, wenn der **Ticketing-E-Mail-Reader** *(siehe 472)* oder ein **Service-Desk**-E-Mail-Reader eine E-Mail von der gleichen E-Mail-Adresse wie das Feld **Kontakt-E-Mail** von **Profil bearbeiten**. Gilt dann, wenn neue E-Mails in den **Ticketing**-E-Mail-Reader kommen, die sich nicht einer der **E-Mail-Mapping** *(siehe 474)* zuordnen lassen, oder wie für **Service-Desk** im Abschnitt "Ticketverknüpfungen" des Themas **Registerkarte "Leseprogramme"** *(http://help.kaseya.com/webhelp/DE/KSD/7000000/index.asp#7560.htm)* in der Online-Hilfe beschrieben.

> **Hinweis:** Wenn mehrere Rechner-IDs dieselbe **Kontakt-E-Mail** haben, kann dieses Kontrollkästchen nur auf einem einzigen Rechner aktiviert sein.

Ansprechpartner

Geben Sie den Namen der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontaktname** angezeigt.

Kontakt-E-Mail

Geben Sie die E-Mail-Adresse der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontakt-E-Mail** angezeigt.

Telefon

Geben Sie die Telefonnummer der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontakt-Telefon** angezeigt.

E-Mail-Administrator

Geben Sie die E-Mail-Adresse ein, unter der dieser verwaltete Rechner Administrator-Support erhält. Diese Einstellunge wird in der Spalte **Admin-E-Mail** angezeigt.

Spracheinstellungen

Die in der Dropdown-Liste **Spracheinstellungen** ausgewählte Sprache legt die Sprache fest, die in einem **Agent-Menü** *(siehe 66)* auf einem verwalteten Rechner angezeigt wird. Die verfügbaren Sprachen werden von den über System > **Voreinstellungen** *(siehe 402)* installierten Sprachpaketen bestimmt.

Rechnerrolle

Die Rechnerrolle, die auf ausgewählte Rechner-IDs angewendet wird. **Rechnerrollen** *(siehe 417)* legen die Funktionen für den **Portalzugriff** *(siehe 75)* fest, die dem Rechnerbenutzer zur Verfügung stehen.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um ausgewählte Rechner-IDs mit den vorher eingegebenen Profilinformationen zu aktualisieren.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Portalzugriff

Agent > Agent konfigurieren> Portalzugriff

Auf der Seite **Portalzugriff** werden der Anmeldename und das Kennwort nach Rechner-ID definiert, damit **Live-Connect** *(siehe 393)* von einem Rechnerbenutzer *remote* verwendet werden kann. Eine von einem Rechnerbenutzer ausgeführte **Live-Connect**-Sitzung wird als **Portalzugriff** bezeichnet. Die über **Portalzugriff** angezeigten Funktionen werden auf der Seite System > Rechnnerrollen > **Zugriffsrechte** *(siehe 418)* festgelegt.

> **Hinweis:** Unter dem ersten Thema der Online-Hilfe können Sie eine Live-Connect-PDF herunterladen.
>
> **Hinweis:** Lesen Sie **Ticketing für Portalzugriffbenutzer auf nicht unterstützten Browsern aktivieren** *(siehe 76)*.

Lokaler Zugriff auf den Portalzugriff

Rechnerbenutzer brauchen sich nicht lokal am **Portalzugriff** anmelden. Durch Klicken auf das Agent-Symbol in der Systemablage Ihres Rechners wird die **Portalzugriffs**-Sitzung ohne Anmeldung eingeleitet.

Remote Zugriff auf die Anmeldeseite des Portalzugriffs

Ein Rechnerbenutzer kann die Anmeldeseite des **Portalzugriffs** für seinen eigenen Rechner von einem anderen Rechner wie folgt anzeigen:

1. Blättern Sie zur Seite `http://your_KServer_address/access/` und ersetzen Sie `your_KServer_address` durch den entsprechenden Ziel-Kaseya Server-Namen im URL-Text.

   > **Hinweis:** Dies ist die gleiche Seite wie die, die VSA-Benutzer zur Anmeldung am VSA verwenden.

2. Melden Sie sich an, indem Sie den Benutzernamen und das Kennwort für den Rechner eingeben. Der Benutzername und das Kennwort werden über die Seite Agent > **Portalzugriff** festgelegt.

   Die Seite **Portalzugriff** wird angezeigt. Der Rechnerbenutzer kann auf jede Menüoption klicken, so als ob er von seinem eigenen verwalteten Rechner aus angemeldet wäre. Er kann auf die Menüoptionen **Desktop** oder **Dateiübertragung** klicken, um eine Remote Verbindung zu seinem eigenen Rechner einzuleiten, ein Ticket zu erstellen oder anzuzeigen oder einen Chat zu beginnen, wenn diese Optionen von der Rechnerrolle aktiviert wurden.

Benutzeranmeldungen neu aktivieren

Anmeldungen von Rechnerbenutzern folgen der gleichen **Anmelderichtlinie** *(siehe 444)* wie VSA-Benutzeranmeldungen. Wenn ein Benutzer versucht, sich zu oft mit dem falschen Kennwort

anzumelden, wird sein Konto automatisch deaktiviert. Sie können die Anmeldung neu aktivieren, indem Sie ein neues Kennwort festlegen oder darauf warten, dass die Deaktivierungszeit für das Konto verstrichen ist.

Portalzugriff anpassen

Portalzugriff-Sitzungen können über System > Anpassen > **Live-Connect** *(siehe 452)* angepasst werden. Es können auch ein Logo, eine Startseite und Links zu anderen URLs hinzugefügt werden.

Login-Name

Geben Sie den **Anmeldenamen** ein, mit dem sich der Benutzer beim VSA anmelden muss, um Chat-Sitzungen einzuleiten, Tickets einzugeben oder anzuzeigen und/oder Fernzugriff auf seinen Rechner zu erhalten. Bei Anmeldenamen und Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Kennwörter müssen mindestens sechs Zeichen lang sein. Der **Anmeldename** wird standardmäßig als Rechner-ID.Gruppen-ID-Name übernommen.

Kennwort erstellen, Kennwort bestätigen

Definieren Sie ein Kennwort für die Anmeldung des Rechnerbenutzers. Kennwörter müssen aus mindestens 6 Zeichen bestehen. Der Rechnerbenutzer kann das Kennwort ändern, nachdem der VSA-Benutzer eins zugewiesen hat.

Anwenden

Klicken Sie auf **Anwenden**, um den Anmeldenamen und das Kennwort für den **Portalzugriff** auf die ausgewählte Rechner-ID anzuwenden.

Löschen

Entfernen Sie die **Anmeldedaten** *(siehe 614)* für den **Portalzugriff** endgültig von der ausgewählten Rechner-ID.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Login-Name

Der dieser Rechner-ID zugewiesene Anmeldename für den **Portalzugriff**

Benutzer-Webanmeldung

Zeigt `Enabled` an, wenn dieser Rechner-ID ein Anmeldename und Kennwort für den **Portalzugriff** zugewiesen wurden. Es zeigt an, dass sich ein Rechnerbenutzer über einen Webbrowser auf einem anderen Rechner *remote* bei der Seite **Portalzugriff** für seinen eigenen Rechner anmelden kann.

Ticketing für Portalzugriffbenutzer auf nicht unterstützten Browsern aktivieren.

Live-Connect und **Portalzugriff** werden auf bestimmten Browsern, die z.B. älter als IE8 oder Firefox 3.5 sind, nicht unterstützt. Rechnerbenutzer, die mit nicht unterstützten Browsern arbeiten müssen, können auf folgendem Weg **Ticketing** *(siehe 456)*-Tickets erstellen und anzeigen:

1. Erstellen Sie eine eigene Rechnerrolle für Benutzer mit nicht unterstützten Browsern in System > **Rechnerrollen** *(siehe 417)*. Erstellen Sie zum Beispiel eine Rechnerrolle `Tickets Only`.
2. Für die neue Rechnerrolle, die Sie soeben erstellt haben, deaktivieren Sie das Kontrollkästchen **Live-Connect** auf der Registerkarte System > Rechnerrollen > **Zugriffsberechtigungen** *(siehe 418)*.
3. Weisen Sie Rechner mit nicht unterstützten Browsern dieser neuen Rechnerrolle zu.

4. Wenn die Rechnerbenutzer ihr Agent-Symbol anklicken, erscheint ein einziges **Ticketing**-Fenster anstelle des Fensters **Portalzugriff**.

> **Hinweis:** Wenn diese Option aktiviert ist, gilt sie für alle Benutzer, die den gleichen verwalteten Rechner verwenden.

Anmeldedaten eingeben

Agent > Agent konfigurieren > Anmeldedaten einstellen

Auf der Seite **Anmeldeinformationen einrichten** werden die erforderlichen Anmeldedaten registriert, damit ein Agent Aufgaben auf Benutzerebene auf einem verwalteten Rechner ausführen kann. Als Anmeldeinformationen bezeichnet man den Anmeldenamen und das Kennwort, die zur Authentifizierung des Zugriffs auf einen Rechner, ein Netzwerk oder eine andere Ressource durch einen Benutzer oder einen Prozess verwendet werden. Die meisten Agent-Aufgaben erfordern keine Anmeldeinformationen. Anmeldeinformationen sind insbesondere erforderlich oder es wird auf sie verwiesen bei:

- Patch-Management – Wenn Anmeldedaten für eine Rechner-ID definiert wurden, installiert **Patch-Management** alle neuen Patches unter Verwendung dieser Anmeldedaten. Daher sollte **Anmeldedaten einstellen** *(siehe 77)* immer *ein Benutzer mit Administratorrechten sein.*
- Patch-Status – Patch-Status setzt die Testergebnisse jedes Mal zurück, wenn **festgelegte Anmeldeinformationen** einer Rechner-ID geändert werden.
- Dateiquelle – Dateiquelle erfordert eventuell, dass festgelegte Anmeldeinformationen als Dateifreigabe für die Rechner-ID definiert werden.
- Patch-Meldung – Richten Sie eine Meldung ein, damit Sie benachrichtigt werden, wenn die Anmeldeinformationen einer Rechner-ID fehlen oder ungültig sind.
- Office-Quelle – Der Agent muss über Anmeldedaten verfügen, um auf den alternativen Office-Speicherort zuzugreifen, falls ein Patch installiert wird, ohne dass ein Benutzer am Rechner angemeldet ist.
- **IF-THEN-ELSE** *(siehe 97)* – Der Befehl `useCredential()` im Agent-Verfahren-Editor erfordert zur erfolgreichen Ausführung, dass Anmeldedaten in **Anmeldedaten einrichten** definiert wurden.
- **Backup** > **Abbildspeicherort** *(http://help.kaseya.com/webhelp/DE/KSD/7000000/index.asp#7948.htm)*– Wenn in **Abbildspeicherort** ein UNC-Pfad angegeben wurde, müssen über **Anmeldedaten einrichten** Anmeldeinformationen definiert werden, die Zugriff auf diesen UNC-Pfad bereitstellen. Ohne die Anmeldedaten hat der Rechner *keinen* Zugriff auf den Abbildspeicherort und die Sicherung schlägt fehl. Stellen Sie beim Angeben eines UNC-Pfads für eine Freigabe, auf die von einem Agent-Rechner zugegriffen wird – zum Beispiel `\\machinename\share` – sicher, dass die Berechtigung der Freigabe Lese-/Schreibzugriff unter Verwendung der Anmeldedaten für diesen Agent-Rechner in > **Anmeldedaten einstellen** *(siehe 77)* zulässt.
- **Ansichtdefinitionen** *(siehe 27)* – Enthält die Option **Rechner mit dem Anmeldestatus**, mit deren Hilfe Sie die Anzeige der Rechner-IDs auf jeder Agent-Seite nach ihrem Anmeldestatus filtern können.
- Desktop Management – Für die Installation des Clients für dieses Modul müssen Anmeldeinformationen definiert sein.

Leere Kennwörter

Leere Kennwörter können verwendet werden, wenn die **lokale Sicherheitsrichtlinie** des verwalteten Rechners dies gestattet. Öffnen Sie auf dem verwalteten Rechner in "Verwaltung" das Tool "Lokale Sicherheitsrichtlinie". Navigieren Sie zu "Lokale Richtlinien – Sicherheitsoptionen". Suchen Sie nach einer Richtlinie namens `Accounts: Limit local account use of blank passwords to console logon only`: Die Standardeinstellung ist aktiviert. Wenn Sie sie in "deaktiviert" ändern, kann ein leeres Kennwort verwendet werden.

Benutzername

Geben Sie den Benutzernamen für die Anmeldeinformationen ein. Normalerweise ist dies ein Benutzerkonto.

Kennwort

Geben Sie das Kennwort ein, das mit dem oben genannten Benutzernamen verknüpft ist.

Domäne

Lokales Benutzerkonto – Wählen Sie diese Option aus, um Anmeldeinformationen für eine lokale Anmeldung an diesem Rechner ohne Verweis auf eine Domäne zu verwenden.

Aktuelle Domäne des Rechners verwenden – Erstellen Sie Anmeldeinformationen unter Verwendung des Namens der Domäne, deren Mitglied dieser Rechner ist. Dies wird vom **letzten Audit** *(siehe 615)* bestimmt. **Alles markieren** erlaubt schnell und einfach einen gemeinsamen Benutzernamen / ein gemeinsames Kennwort auf mehreren Rechnern einzurichten, selbst wenn ausgewählte Rechner verschiedenen Domänen angehören.

Domäne angeben – Geben Sie den Domänennamen manuell an, der für diese Anmeldeinformationen verwendet werden soll.

Anwenden

Weisen Sie die Anmeldeinformationen allen markierten Rechner-IDs zu. Rechner-IDs mit zugewiesenen Anmeldeinformationen zeigen den Benutzernamen und die Domäne in den entsprechenden Tabellenspalten an.

Löschen

Entfernen Sie die Anmeldeinformationen von allen markierten Rechner-IDs.

Test

Klicken Sie auf **Test**, um zu überprüfen, ob Benutzername/Kennwort/Domänen-Anmeldedaten funktionieren, bevor Sie sie einer Rechner-ID zuweisen.

Abbrechen

Klicken Sie auf **Abbrechen**, um das Testen der Benutzername/Kennwort/Domänen-Anmeldedaten abzubrechen.

LAN-Cache

Agent > Agent konfigurieren > LAN-Cache

Die Seite **LAN-Cache** designiert einen Rechner so, dass er als Dateiquelle für andere Rechner auf dem gleichen LAN agiert. Wenn ein LAN-Cache aktiviert ist und ein Rechner im gleichen LAN zum ersten Mal einen Download vom Kaseya Server anfordert, werden die Dateien auf den LAN-Cache-Rechner heruntergeladen und dann auf den anfordernden Rechner kopiert. Ab dem Zeitpunkt muss die Datei nicht mehr vom Kaseya Server heruntergeladen werden. Andere Rechner – auf dem gleichen LAN mit dem gleichen LAN-Cache – kopieren die Datei aus dem LAN-Cache-Rechner. Dadurch werden die Zustellung an mehrere Rechner im gleichen LAN beschleunigt und Probleme mit der Netzwerkbandbreite reduziert.

Hintergrund

LAN-Cache konfiguriert eine Dateiquelle wie folgt:

- Erstellt automatisch ein lokales Administrator- oder Domänen-Administratorkonto oder ermöglicht Ihnen, die Anmeldedaten für einen vorhandenen Domänen-Administrator manuell anzugeben.   Erstellte Konten erhalten einen eindeutigen Namen (`FSAdminxxxxxxxxx`, wobei `x`

eine Ziffer ist) mit einem automatisch generierten starken Kennwort. Das generierte Kennwort enthält 15 zufällig ausgewählte Zeichen, davon mindestens eines der folgenden Zeichen:

- Großbuchstaben
- Kleinbuchstaben
- Zahlen (0–9)
- Nicht-alphanumerische Zeichen

- Sobald das Kennwort erstellt wurde, wird es mit dem Adminnamen verglichen, um sicherzustellen, dass keine zwei Zeichenkombinationen im Kennwort mit zwei Zeichenkombinationen im Adminnamen übereinstimmen. Durch diese Logik wird sichergestellt, dass die generierten Kennwörter jeder Komplexitätslogik für Windows-Kennwörter entsprechen.
- Die Anmeldedaten für das Konto werden mit diesem LAN-Cache innerhalb von Kaseya verbunden und bei Bedarf anstatt von zugeordneten Agent-Anmeldedaten verwendet. *LAN-Cache erfordert und unterstützt nicht die Verwendung der auf der Seite "Anmeldedaten erstellen" angegebenen Anmeldedaten.*
- Erstellen des angegebenen Kundenfreigabeverzeichnisses auf dem angegebenen festen Laufwerk, das als Windows-Verwaltungsfreigabe konfiguriert ist. Das Verzeichnis und die Freigabe werden erstellt, ohne dass die Seite **LAN-Cache** verlassen werden muss. Das für den LAN-Cache angegebene Verzeichnis ist ausschließlich für die Kundenverwendung gedacht. *Kaseya verwendet dieses vom Kunden angegebene Verzeichnis/diese Freigabe nie.*
- Erstellen eines speziellen Kaseya-Verzeichnisses – immer `VSAFileShare` als Unterverzeichnis unter dem Kundenverzeichnis – auf dem angegebenen festen Laufwerk, das als Windows-Verwaltungsfreigabe konfiguriert ist.

Verfahren – Allgemein

1. Wählen Sie einen LAN-Cache-Rechner.
2. Weisen Sie Rechner über die Seite **LAN-Cache zuweisen** *(siehe 81)* dem LAN-Cache zu.

Verfahren – Für writeFile()- und getURL()-Schritte in Agent-Verfahren

Mit diesen Befehlen können Dateien von einem **LAN-Cache** anstatt von einem VSA oder einer URL heruntergeladen werden. Die Dateien müssen größer als 4 kB sein.

1. Wählen Sie einen LAN-Cache-Rechner.
2. Weisen Sie Rechner über die Seite **LAN-Cache zuweisen** *(siehe 81)* dem LAN-Cache zu.
3. Laden Sie *nur beim writeFile()-Befehl* die Dateien hoch, die Sie auf zugeordnete Rechner auf den Kaseya Server mit dem Ordner Agent-Verfahren > Verfahren verwalten > Planen/Erstellen > **Dateien verwalten** *(siehe 124)* > *Gemeinsam genutzt* herunterladen möchten. Die Dateien müssen größer als 4 kB sein.
4. Erstellen und führen Sie ein Agent-Verfahren aus, das einen **writeFile()** *(siehe 118)*- oder **getURL()** *(siehe 110)*-Schritt enthält.
    - Wenn ein Agent den Schritt **writeFile()** oder **getURL()** eines Agent-Verfahrens zum ersten Mal ausführt, wird die Datei vom KServer oder der URL heruntergeladen und dann wird der zugeordnete LAN-Cache mit der Datei aktualisiert.
    - Für nachfolgende Anforderungen für die gleiche Datei von einem beliebigen Agent wird die Datei vom LAN-Cache und nicht von ihrer ursprünglichen Quelle heruntergeladen.
    - Um den Caching-Mechanismus vollständig nutzen zu können, führen Sie zuerst das Agent-Verfahren aus, das die Datei auf einen Agent verweist. Nachdem dieser Agent die Datei in den zugeordneten LAN-Cache hochgeladen hat, führen Sie dieses Verfahren mit anderen Agents aus, die dem gleichen LAN-Cache zugeordnet sind.

Aktionen

- **LAN-Cache hinzufügen** – Gibt einen LAN-Cache auf einem ausgewählten Rechner an.

- **1. LAN-Cache-Name** – Geben Sie einen Namen auf dem LAN-Cache an, wie er in **LAN-Cache zuordnen** angezeigt wird.
- **2. Verzeichnisname** – Geben Sie nur den Namen des Verzeichnisses an, ohne den Namen des Rechners oder den Laufwerksbuchstaben anzugeben. Das Verzeichnis muss nicht bereits vorhanden sein. Der LAN-Cache erstellt das Verzeichnis und die erforderlichen Freigabeeinstellungen für Sie.
- **3. Wählen Sie die UNC-Servernamenauflösung** – **Verwenden Sie den Computernamen** oder die **Computer-IP-Adresse**. Gibt das für den Zugriff auf die Freigabe verwendete UNC-Namenauflösungsformat an. Beispiel: `\\computername\sharename$` oder `\\10.10.10.118\sharename$`.

> **Hinweis:** Der nächste Schritt, die Auswahl des Anmeldetypen, wird nicht angezeigt, wenn die Option System > **Standardeinstellung** *(siehe 437)* > **LAN-Cache – Automatisch erstellte Administrator-Anmeldedaten verwenden** auf "Ja" gesetzt ist.

- **4. Wählen Sie den zu verwendenden Typ der LAN-Cache-Administrator-Anmeldedaten aus.**
  - ✓ **Automatisch erstellte Administrator-Anmeldedaten verwenden** – Wenn diese Option aktiviert ist, werden Administrator-Anmeldedaten für Sie erstellt, wenn der LAN-Cache erstellt wird. Es werden lokale Administrator-Anmeldedaten erstellt, es sei denn, der Rechner ist ein Domain-Controller. Wenn der Rechner ein Domain-Controller ist, werden Domänen-Administratoranmeldedaten erstellt.
  - ✓ **Vorhandene Domänen-Administratoranmeldedaten verwenden** – Wenn diese Option aktiviert ist, geben Sie die Domäne, den Benutzernamen und das Kennwort vorhandener Domänen-Anmeldedaten ein. Die Domänen-Anmeldedaten werden nicht erstellt.
- **5. Wählen Sie ein festes Laufwerk aus, auf dem der LAN-Cache erstellt wird.** – Wählen Sie das Laufwerk aus, auf dem die Freigabe erstellt wird.

- **LAN-Cache entfernen** – Entfernt den LAN-Cache aus einem ausgewählten Rechner.
- **Ausstehendes löschen** – Storniert die ausstehende Erstellung eines LAN-Cache auf einem ausgewählten Rechner.
- **Generierte Cache-Anmeldedaten testen** – Klicken Sie auf diese Option, um die von einem ausgewählten Rechner verwendeten Anmeldedaten zu testen. Das Ergebnis wird in der Spalte **Teststatus der Anmeldedaten** angezeigt.

Spalten

- **(Check-in-Symbol) –** Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **Rechner.Gruppen-ID** – Ein eindeutiger **Rechner-ID/Gruppen-ID-/Organisations-ID-** *(siehe 626)*Name für einen Rechner im VSA.
- **Cache-Name** – Der Name des LAN-Cache, wie mit dem VSA angezeigt.
- **Cache-Pfad** – Der für den LAN-Cache angegebene Pfad.
- **Cache-UNC** – Der für die Lokalisierung des LAN-Cache im Netzwerk verwendete UNC.
- **Cache erstellt** – Datum/Uhrzeit, an dem bzw. zu der der LAN-Cache erstellt wurde.

- **Cache-Administrator** – Das für den Zugriff auf den LAN-Cache verwendete Administratorkonto.
- **Teststatus der Anmeldedaten** – Zeigt die Ergebnisse der Tests der Administrator-Kontoanmeldedaten an, die für den Zugriff auf den LAN-Cache verwendet werden. Anmeldedaten können über die Schaltfläche **Generierte Cache-Anmeldedaten testen** oben auf der Seite getestet werden.

LAN-Cache zuweisen

Agent > Agent konfigurieren > LAN-Cache zuweisen

Auf der Seite **LAN-Cache zuweisen** werden Rechner einem ausgewählten **LAN-Cache** *(siehe 78)*-Rechner zugewiesen bzw. daraus entfernt.

Aktionen

- **Zuweisen** – Weist einen aus der Dropdown-Liste ausgewählten LAN-Cache ausgewählten Rechnern zu.
- **Zuweisen aufheben** – Hebt die Zuweisung eines LAN-Cache zu ausgewählten Rechnern auf.
- **Ausstehendes löschen** – Storniert die ausstehende Zuweisung eines LAN-Cache zu einem ausgewählten Rechner.
- **Generierte Cache-Anmeldedaten testen** – Klicken Sie auf diese Option, um die von einem ausgewählten Rechner verwendeten Anmeldedaten zu testen. Das Ergebnis wird in der Spalte **Teststatus der Anmeldedaten** angezeigt.

Spalten

- **Alle auswählen/Alle abwählen** – Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.
- **Rechner.Gruppen-ID** – Ein eindeutiger **Rechner-ID/Gruppen-ID-/Organisations-ID-** *(siehe 626)*Name für einen Rechner im VSA.
- **Zugewiesener LAN-Cache** – Zeigt den LAN-Cache an, dem ein Rechner zugewiesen ist.
- **Zugewiesen** – Das Datum/die Uhrzeit, an dem ein Rechner einem LAN-Cache zugewiesen wurde.
- **Teststatus** – **Test Status der Anmeldedaten** – Zeigt die Ergebnisse der Tests der Administrator-Kontoanmeldedaten an, die für den Zugriff auf den LAN-Cache verwendet werden. Anmeldedaten können über die Schaltfläche **Generierte Cache-Anmeldedaten testen** oben auf der Seite getestet werden.

Agent aktualisieren

Agent > Version aufrüsten > Agent aktualisieren

Auf der Seite **Agent aktualisieren** wird geplant, verwaltete Rechner mit der neuesten Version der Agent-Software beider nächsten Anmeldung des Agents zu aktualisieren. Die für jeden Agent definierten **Agent-Einstellungen** *(siehe 611)* werden durch diese Aktualisierung nicht geändert.

> **Hinweis:** Alle für die Überwachung verwendeten Agents müssen über die Seite Agent > Agent aktualisieren aktualisiert werden.

Agent aktualisieren

Klicken Sie auf **Agent aktualisieren**, um die Aktualisierung ausgewählter Rechner zu planen.

Beim Login daran erinnern, wenn Agents ein Update benötigen

Wenn dies markiert ist, wird bei der Anmeldung von VSA-Benutzern ein Popup-Fenster angezeigt, wenn verwaltete Rechner unter ihrer Kontrolle mit der letzten Version der Agent-Software aktualisiert werden müssen. Diese Erinnerungsmeldung wird nur angezeigt, wenn mindestens ein Agent innerhalb des **Scopes** *(siehe 419)* des VSA-Benutzers aktualisiert werden muss. Benutzer können diese Funktion zum Zeitpunkt der Anmeldung deaktivieren und durch Markieren dieses Kontrollkästchens erneut aktivieren.

Update erzwingen, selbst wenn Agent-Version x.x.x.x. ist

Wenn dies aktiviert ist, werden die für die Aktualisierung ausgewählten Rechner mit neuen Dateien aktualisiert, die die Agent-Dateien auf dem verwalteten Rechner ersetzen, selbst wenn die Agent-Version gegenwärtig aktuell ist. Es wird eine "saubere" Installation der Agent-Dateien ausgeführt.

Nach der Aktualisierung über <Agent-Verfahren auswählen> Agent-Verrfahren ausführen

Wählen Sie ein Agent-Verfahren aus, das sofort nach Abschluss der Fertigstellung eines Agents ausgeführt werden soll. Mit dieser Funktion können Sie Anpassungen erneut auf einen Agent anwenden, die eventuell nach der Agent-Aktualisierung verloren gehen. Normalerweise umfassen diese Anpassungen das Ausblenden oder Umbenennen von Agent-Bezeichnern auf verwalteten Rechnern, damit Benutzer nicht erkennen, dass der Agent überhaupt installiert ist.

Update abbrechen

Klicken Sie auf **Update abbrechen**, um eine anstehende Aktualisierung auf ausgewählten verwalteten Rechnern abzubrechen.

Herunterladen des Live Connect-Plugin-Installationsprogramms für Windows-Browser

Bei allen Versionen von Windows, die von Live Connect unterstützt werden, wird durch Klicken auf diesen Link ein eigenständiges Installationsprogramm auf den lokalen Rechner des VSA-Benutzers heruntergeladen. Das Installationsprogramm installiert den Live Connect-Plugin Manager und alle Live Connect-Plugins für Chrome, Firefox und Internet Explorer.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Agentversion

Die Version der Agent-Software, die auf dem verwalteten Rechner ausgeführt wird. Versionsnummern in rot deuten darauf hin, dass die Version auf dem Agent-Rechner nicht dieselbe wie die aktuellste verfügbare Version ist.

Agent-Verfahren aktualisieren

Dies ist das Agent-Verfahren, das bei der Aktualisierung des Agents ausgeführt werden soll.

Letztes Update

Das Datum, an dem der Agent zuletzt auf dem verwalteten Rechner aktualisiert wurde. Da der Server auf einen Check-in des verwalteten Rechners warten muss (wie in Agent > **Check-in-Kontrolle** *(siehe 68)* angegeben), wird `Pending` in der Spalte **Letztes Update** angezeigt, bis der nächste Check-in eintritt.

Dateizugriff

Agent > Schutz > Dateizugriff

Über die Seite **Dateizugriff** kann der unautorisierte Zugriff auf Dateien auf verwalteten Rechnern durch Rogue-Anwendungen oder Benutzer verhindert werden. Jeder Anwendung kann der Zugriff auf die Datei gewährt oder verweigert werden.

> **Hinweis:** Sie können auch den Betriebssystemzugriff auf die geschützte Datei blockieren, indem Sie den Zugriff auf `explorer.exe` und/oder `cmd.exe` blockieren. Dadurch wird verhindert, dass die Datei umbenannt, verschoben oder gelöscht wird und damit jede Verfälschung der Datei unterbunden wird.

Mehrere Agents

Wenn **mehrere Agents** *(siehe 50)* auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 83)*, **Netzwerkzugriff** *(siehe 84)* und **Anwendungsblocker** *(siehe 88)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese Treiber kontrolliert.

Blockieren

Wenn Sie den unautorisierten Zugriff auf eine Datei durch Rogue-Anwendungen verhindern wollen, geben Sie den Dateinamen ein und klicken Sie auf die Schaltfläche **Blockieren** . Dadurch wird das Popup-Fenster **Dateizugriff** eingeblendet.

In diesem Dialog kann der Benutzer zwischen folgenden Optionen wählen:

- **Dateiname für Zugriffskontrolle** – Geben Sie den **Dateinamen und/oder einen Teil des vollständigen Pfads** ein. Wenn Sie beispielsweise den Dateinamen `protectme.doc` zu der Liste hinzufügen, werden alle Vorkommnisse von `protectme.doc` in allen Verzeichnissen und auf jedem Laufwerk geschützt. Durch Hinzufügen von `myfolder\protectme.doc` werden alle Vorkommnisse der Datei in allen Verzeichnissen namens `myfolder` geschützt.
- **Neu** – Fügen Sie eine neue Anwendung zu der Zugriffsliste hinzu. Sie können die Anwendungen manuell eingeben oder mithilfe der Schaltfläche **Suchen...** einen Anwendungsnamen auswählen.
- **Entfernen** – Entfernen Sie eine Anwendung aus der Zugriffsliste.
- **Suchen** – Wählen Sie eine Rechner-ID aus, um die Liste der auf dieser Rechner-ID installierten Anwendungen zu durchsuchen, und wählen Sie anschließend einen Anwendungsnamen aus. Diese Liste basiert auf der letzten Inventarisierung, die für diese Rechner-ID durchgeführt wurde. Sie durchsuchen nicht wirklich den verwalteten Rechner.
- **Benutzer fragen, die nicht aufgelisteten freizugeben** – Damit wird dem Benutzer die Möglichkeit gegeben, den Zugriff auf die Datei auf Anwendungsbasis jedes Mal zu gewähren oder zu

verweigern, wenn eine neue Anwendung versucht, auf diese Datei zuzugreifen. Anhand dieser Funktion können Sie die Zugriffsliste basierend auf der normalen Nutzung aufbauen.

- **Alle nicht aufgelisteten ablehnen** – Blockiert alle Anwendungen vom Zugriff auf die Datei. Wählen Sie diese Option, wenn Sie sich nicht sicher sind, für welche Dateien Zugriff benötigt wird und für welche nicht.

Entsperren

Entfernen Sie eine Anwendung aus der Schutzliste, indem Sie auf die Schaltfläche **Entsperren** klicken. Dadurch wird ein neues Dialogfeld geöffnet, in dem alle geschützten Dateien für die ausgewählten Rechner-IDs ausgewählt werden. Sie können Dateien von dem ausgewählten Rechner oder von allen Rechnern mit diesem Dateipfad entfernen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Dateiname

Dateiname der zu blockierenden Datei. Klicken Sie auf das Bearbeitungssymbol neben einem Dateinamen, um die Dateizugriffsberechtigungen für diesen Dateinamen zu ändern.

Bestätigte Anwendungen

Hier werden die Anwendungen aufgelistet, für die der Zugriff auf die Datei auf dieser Rechner-ID bestätigt wurde.

Benutzer um Bestätigung bitten

Wenn diese Option aktiviert ist, wird der Benutzer einer Rechner-ID gefragt, ob er den Dateizugriff bestätigen will, wenn eine nicht zugelassene Anwendung versucht, auf die Datei zuzugreifen.

Netzwerkzugriff

Agent > Schutz > Netzwerkzugriff

Über die Seite **Netzwerkzugriff** können Sie den **TCP/IP-Protokoll-basierten Netzwerkzugriff** auf Anwendungsbasis bestätigen oder verweigern. Benutzer können ebenfalls benachrichtigt werden,

wenn nicht eine aufgelistete Anwendung auf das Netzwerk zugreift, und dieser Anwendung den Netzwerkzugriff bestätigen oder verweigern. Über diese Funktion wird in der Regel der Zugriff auf interne und externe *Internet*-Sites gesteuert. Dies kann jedoch auch internen LAN-Verkehr, der das TCP/IP-Protokoll verwendet, einschließen.

Treiber

Diese Funktion erfordert, dass der Treiber *aktiviert*wird, den Netzwerkzugriff zu blockieren und die Bandbreitenstatistiken des Netzwerks zu überwachen. Dieser Treiber ist standardmäßig *deaktiviert*. Dieser Treiber fügt sich in den TCP/IP-Stapel ein, um den auf dem TCP/IP-Protokoll basierenden Datenverkehr nach Anwendung zu messen. *Bei Windows-Rechnern, die mit einem älteren Betriebssystem als Vista laufen, wird ein aktivierter Rechner erst nach einem Neustart des Rechners aktiv.*

Hinweis: Um festzustellen, welchen Anwendungen der Netzwerkzugriff bestätigt oder verweigert werden soll, zeigen Sie über den Bericht **Netzwerkstatistiken** *(siehe 208)* die Netzwerkbandbreitennutzung während eines bestimmten Zeitraums an. Klicken Sie auf die Datenpunkte des Diagramms, um weitere Details anzuzeigen und die Top-Verbraucher von Bandbreite zu identifizieren. Stellen Sie fest, welche Anwendung und welcher Rechner zu einem gegebenen Zeitpunkt Bandbreite verbraucht.

Warnung: Anwendungen, die den Windows TCP/IP-Stapel nicht auf normale Weise verwenden, können Konflikte mit dem Treiber verursachen, der zum Erfassen von Informationen und Blockieren des Zugriffs verwendet wird. Dies gilt insbesondere für ältere Anwendungen.

Mehrere Agents

Wenn **mehrere Agents** *(siehe 50)* auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 83)*, **Netzwerkzugriff** *(siehe 84)* und **Anwendungsblocker** *(siehe 88)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese Treiber kontrolliert.

So bestätigen oder verweigern Sie den Netzwerkzugriff für eine oder mehrere Anwendungen

1. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Rechner-IDs in der Spalte **Rechner.Gruppen-ID**.
2. Klicken Sie auf den Link einer *beliebigen* Rechner-ID in der Spalte **Rechner.Gruppen-ID**. Dies braucht nicht unbedingt die Rechner-ID zu sein, die Sie markiert haben. Dadurch wird das Popup-Fenster **Anwendungsliste** mit allen auf dieser Rechner-ID installierten Anwendungen eingeblendet. Diese Liste basiert auf der letzten Inventarisierung, die für diese Rechner-ID durchgeführt wurde.
3. Da die im Fenster **Anwendungsliste** angezeigte Liste sehr umfangreich sein kann, sollten Sie sie durch Klicken auf **Filter** filtern und so die Anzeige der Dateien besser steuern.
4. Aktivieren Sie die Kontrollkästchen neben dem Namen der Anwendung, der Sie Netzwerkzugriff bestätigen oder verweigern möchten.
5. Sie können auch Anwendungsnamen in das Bearbeitungsfeld **Anwendungen, die bei Audit nicht gefunden wurden, hier hinzufügen** eingeben, um nicht aufgelistete Anwendungen zu identifizieren.
6. Klicken Sie auf die Schaltfläche **Auswählen**, um Ihre Auswahlen zu bestätigen und das Fenster **Anwendungsliste** zu schließen. Die ausgewählten Anwendungen werden jetzt am Anfang der Seite angezeigt.
7. Klicken Sie auf **Anwendungen bestätigen** oder **Anwendungen ablehnen**. Die im Fenster **Anwendungsliste** ausgewählten Anwendungen werden zur Spalte **Bestätigte/Abgelehnte Anwendungen** hinzugefügt.

So entfernen Sie die Einstellungen für Bestätigung und Ablehnung für eine oder mehrere Rechner-IDs

1. Aktivieren Sie das Kontrollkästchen neben einer oder mehreren Rechner-IDs in der Spalte **Rechner.Gruppen-ID**.
2. Klicken Sie auf die Schaltfläche **Anwendungen entfernen**.

Optionen für Netzwerkzugriff

- **Benutzer benachrichtigen, wenn Anwendung geblockt ist** – Benutzer benachrichtigen, wenn eine geblockte Anwendung auf das Netzwerk zugreifen will. Anhand dieser Funktion können Sie die Zugriffsliste basierend auf der normalen Nutzung aufbauen. Auf diese Weise können Sie sehen, welche Anwendungen auf Ihrem System auf das Netzwerk zugreifen und wann. Der Rechnerbenutzer ist aufgefordert eine von vier Antworten zu wählen, wenn eine Anwendung geblockt ist:
  - **Immer** – Gewährt der Anwendung unbegrenzt den Zugriff auf das Netzwerk. Die Benutzer werden nicht erneut aufgefordert.
  - **Ja** – Der Anwendung wird der Zugriff auf das Netzwerk für die Dauer der Sitzung gewährt. Die Benutzer werden erneut aufgefordert.
  - **Nein** – Der Anwendung wird der Zugriff auf das Netzwerk für die Dauer der Sitzung verweigert. Die Benutzer werden erneut aufgefordert.
  - **Nie** – Verweigert der Anwendung immer den Zugriff auf das Netzwerk. Die Benutzer werden nicht erneut aufgefordert.
- **Treiber bei nächstem Neustart aktivieren/deaktivieren** – den Netzwerkzugriff-Protection-Treiber für einen Agent **Aktivieren/Deaktivieren**. Anwendungen, die den Windows TCP/IP-Stapel nicht auf normale Weise verwenden, können Konflikte mit diesem Treiber verursachen. Dies gilt insbesondere für ältere Anwendungen. **Der Agent kann keine Netzwerkstatistiken überwachen oder den Netzwerkzugriff blockieren, wenn der Treiber deaktiviert ist.** *Bei Windows-Rechnern, die mit einem älteren Betriebssystem als Vista laufen, wird ein aktivierter Rechner erst nach einem Neustart des Rechners aktiv.*
- **Nicht gelistete Aktion anwenden** – Bei einer nicht gelisteten Anwendung handelt es sich um eine Anwendung, für die der Zugriff auf das Netzwerk nicht ausdrücklich gewährt oder verweigert wurde. Geben Sie an, was unternommen werden soll, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen.
  - **Benutzer bitten, die nicht gelisteten freizugeben** – Ein Bestätigungsdialogfeld wird angezeigt, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen.
  - **Alle nicht gelisteten freigeben** – Der nicht gelisteten Anwendung wird der Zugriff auf das Netzwerk gewährt.
  - **Alle nicht gelisteten ablehnen** – Der nicht gelisteten Anwendung wird der Zugriff auf das Netzwerk verweigert, und die Anwendung wird auf dem verwalteten Rechner geschlossen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Benutzer benachrichtigen

Ein grünes Häkchen ✓ in der Spalte **Benutzer benachrichtigen** weist darauf hin, dass der Benutzer des verwalteten Rechners benachrichtigt wird, wenn eine Anwendung versucht, auf das Netzwerk zuzugreifen, der der Netzwerkzugriff verweigert wurde.

So benachrichtigen Sie den Benutzer, wenn eine Anwendung abgelehnt wurde:

1. Wählen Sie die Rechner-IDs aus.
2. Klicken Sie auf die Schaltfläche **Aktivieren** für **Benutzer benachrichtigen, wenn die Anwendung blockiert ist**.

So entfernen Sie diese Benachrichtigung:

1. Wählen Sie die Rechner-IDs aus, für die ✓ in der Spalte **Benachrichtigen** ein grünes Häkchen angezeigt wird.
2. Klicken Sie auf die Schaltfläche **Deaktivieren** für **Benutzer benachrichtigen, wenn die Anwendung blockiert ist**.

Treiber aktivieren

Identifiziert auf Rechner-ID-Basis, für welche Rechner der Netzwerkschutztreiber aktiviert wurde oder nicht. *Bei Windows-Rechnern, die mit einem älteren Betriebssystem als Vista laufen, wird ein aktivierter Rechner erst nach einem Neustart des Rechners aktiv.*

Nicht aufgelistete Aktion

Zeigt die **nicht gelistete Aktion** an, die ausgeführt werden soll, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen. Siehe **Nicht gelistete Aktion anwenden** weiter oben.

Bestätigte Anwendungen / Lehnt Anwendungen ab / Anwendungen entfernen / Alle entfernen

Diese Einstellungen können erst angewendet werden, wenn der Treiber aktiviert ist.

- Bestätigte Anwendungen werden in der ersten Zeile gelistet.
- Abgelehnte Anwendungen werden in der zweiten Zeile gelistet.
- Falls das Optionsfeld **Alle nicht gelisteten bestätigen** ausgewählt ist und auf eine Rechner-ID angewendet wurde, wird die Liste der bestätigten Anwendungen durch den Ausdruck `Approve All Unlisted` ersetzt.
- Falls das Optionsfeld **Alle nicht aufgelisteten ablehnen** ausgewählt ist und auf eine Rechner-ID angewendet wurde, wird die Liste der bestätigten Anwendungen durch den Ausdruck `Deny All Unlisted` ersetzt.
- Klicken Sie auf **Anwendungen entfernen**, um ausgewählte Anwendungen von ausgewählten Rechner zu entfernen.
- Klicken Sie auf **Anwendungen entfernen**, um ausgewählte Anwendungen von ausgewählten Rechner zu entfernen.

Anwendungsblocker

Agent > Schutz > Anwendungsblocker

Über die Seite **Anwendungsblocker** kann verhindert werden, dass beliebige Anwendungen auf einer Rechner-ID ausgeführt werden. Blockierte Anwendungen können weder umbenannt noch verschoben oder vom System gelöscht werden. **Dateizugriff** *(siehe 83)* kann auch Anwendungen blockieren, **Anwendungsblocker** kann jedoch schneller konfiguriert werden, wenn Sie Anwendungen einfach nur blockieren bzw. die Blockierung aufheben möchten.

Mehrere Agents

Wenn **mehrere Agents** *(siehe 50)* auf einem Rechner installiert sind, kontrolliert jeweils nur ein Agent die Treiber, die zur Verwendung von **Dateizugriff** *(siehe 83)*, **Netzwerkzugriff** *(siehe 84)* und **Anwendungsblocker** *(siehe 88)* erforderlich sind. Diese Funktionen können nur von dem Agent ausgeführt werden, der diese Treiber kontrolliert.

Blockieren

So blockieren Sie das Ausführen einer Anwendung auf einem Rechner:

1. Wählen Sie eine oder mehrere Rechner-IDs aus. Nur Rechner-IDs, die aktuell dem **Rechner-ID/Gruppen-ID-Filter** *(siehe 26)* entsprechen, werden angezeigt.
2. Geben Sie den Dateinamen der Anwendung in das Bearbeitungsfeld ein.

   Die Anwendung kann **durch ihren Dateinamen und/oder einen Teil des vollständigen Pfads referenziert werden**. Beispiel: Durch Hinzufügen einer Anwendung namens `blockme.exe` zu der Liste wird die Ausführung aller Vorkommnisse von `blockme.exe` in jedem Verzeichnis und auf jedem Laufwerk verhindert. Wenn Sie `myfolder\blockme.exe` hinzufügen, wird die Ausführung aller Vorkommnisse der Anwendung in allen Verzeichnissen namens `myfolder` verhindert.
3. Klicken Sie auf die Schaltfläche **Blockieren** .
4. Die blockierte Anwendung wird in der Spalte **Anwendung** neben den ausgewählten Rechner-IDs angezeigt.

Entsperren

So entsperren Sie eine Anwendung in der Liste der blockierten Anwendungen:

1. Wählen Sie eine oder mehrere Rechner-IDs aus, die blockierte Anwendungen in der Spalte **Anwendung** aufführen.
2. Klicken Sie auf die Schaltfläche **Entsperren**. Ein Popup-Fenster **Dateizugriff** wird geöffnet, in dem alle blockierten Anwendungen für die ausgewählten Rechner-IDs aufgelistet sind.
3. Klicken Sie auf eine oder mehrere blockierte Anwendungen.
4. Klicken Sie auf die Schaltfläche **Entsperren**. Das Fenster wird geschlossen.
5. Die blockierte Anwendung wird nicht länger in der Spalte **Anwendung** neben den ausgewählten Rechner-IDs angezeigt.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Anwendung

Der Dateiname der blockierten Anwendung.

Kapitel 4

Skripting

In diesem Kapitel

Überblick über Agent-Verfahren

Skripting

Das Modul **Agent-Verfahren erstellt und verwaltet Agent-Verfahren** *(siehe 92)* auf verwalteten Rechnern. Unter Verwendung von **Agent-Verfahren-Status** *(siehe 127)* können Sie den Status sämtlicher Verfahren anzeigen, die auf einem verwalteten Rechner ausgeführt werden. Mit **Verteilung** *(siehe 126)* können Sie außerdem die Auswirkung von Agent-Verfahren auf den Datenverkehr und die Serverlast ausgleichen.

Das Modul **Agent-Verfahren** bietet darüber hinaus folgende Funktionen:

- **Dateiübertragungen** – Überträgt Dateien auf und von verwalteten Rechnern mit **Datei abrufen** *(siehe 134)* und **Datei verteilen** *(siehe 135)*.
- **Benutzerdefinierte Installationen** – Wenn keine vordefinierte Installationslösung verwendet werden kann, erstellen Sie mithilfe des **Packager** *(siehe 133)* eine selbstextrahierende Datei zur automatisierten Verteilung.
- **Verteilung von Patches und Anwendungen** – Sie können die Installation von Anwendungen und Patches von Microsoft und anderen Herstellern mithilfe von **Patch-Bereitstellung** *(siehe 129)* und **Anwendungsbereitstellung** *(siehe 130)* planen.

Hinweis: Informationen zur Installation von Microsoft-Patches auf verwalteten Rechnern finden Sie unter Patch-Management.

Funktionen	Beschreibung
Planen/Erstellen *(siehe 92)*	Automatisiert benutzerdefinierte Aufgaben auf verwalteten Rechnern, indem Agent-Verfahren erstellt und geplant werden.
Verteilung *(siehe 126)*	Reduziert den Netzverkehr und die Serverlast, indem Agent-Verfahren gleichmäßig über den Tag verteilt ausgeführt werden.
Skripting-Status *(siehe 127)*	Zeigt den Status der Agent-Verfahren an, die auf verwalteten Rechnern ausgeführt werden.
Patch-Bereitstellung *(siehe 129)*	Mit diesem Assistenten können Sie Verfahren zur Bereitstellung von Microsoft-Patches auf verwalteten Rechnern erstellen.
Anwendungsbereitstellung *(siehe 130)*	Mit diesem Assistenten können Sie Verfahren zur Bereitstellung von anderen Patches als von Microsoft auf verwalteten Rechnern erstellen.
Objekt-Manager *(siehe 133)*	Dies ist eine externe Anwendung, mit der Benutzer angepasste Installationspakete zur Bereitstellung auf verwalteten Rechnern erstellen.
Datei abrufen *(siehe 134)*	Unter Verwendung des Agent-Verfahrensbefehls "getFile()" können Dateien, die von verwalteten Rechnern auf den Kaseya Server hochgeladen wurden, angezeigt und verwaltet werden.
Datei verteilen *(siehe 135)*	Schreiben Sie Dateien auf alle ausgewählten verwalteten Rechner und pflegen Sie sie.

Planen/Erstellen

Agent-Verfahren > Verfahren verwalten > Planen/Erstellen

Auf der Seite **Planen/Erstellen** werden benutzerdefinierte Aufgaben auf verwalteten Rechnern durch

Planung und Erstellung von *Agent-Verfahren* automatisiert. Nähere Informationen erhalten Sie in den folgenden Themen:

- **Aktionsschaltflächen** *(siehe 93)*
- **Agent-Verfahren planen** *(siehe 94)*
- **Agent-Verfahren erstellen/bearbeiten** *(siehe 95)*
- **IF-ELSE-Schritt-Befehle** *(siehe 97)*
- **64-Bit-Befehle** *(siehe 119)*
- **Variablen verwenden** *(siehe 120)*
- **Variable Manager** *(siehe 123)*
- **Auf dem Server gespeicherte Dateien verwalten** *(siehe 124)*
- **Ordnerrechte** *(siehe 125)*

Verwandte Themen

- **Meldungen bei Fehlschlagen des Agent-Verfahrens** – Die Seite **Meldungen – Fehlgeschlagene Agent-Verfahren** *(siehe 299)* löst eine Meldung aus, wenn die Ausführung eines Agent-Verfahrens auf einem verwalteten Rechner fehlschlägt. Wenn Sie beispielsweise einen Dateinamen, Verzeichnispfad oder Registrierungsschlüssel in einem Agent-Verfahren angeben und das Verfahren dann auf einer Rechner-ID ausführen, für die diese Werte ungültig sind, können Sie unter Verwendung dieser Seite darüber benachrichtigt werden.
- **Fehlgeschlagene Schritte in Verfahren protokollieren** – Die Seite "System > **Konfigurieren** *(siehe 429)*" enthält die Option **Protokollierung von Verfahrensfehlern mit Markierung "Verfahren fortsetzen, falls Schritt fehlschlägt" aktivieren**. Wenn diese Option aktiviert ist, werden fehlgeschlagene Schritte in Verfahren protokolliert. Ist diese Option nicht aktiviert, werden fehlgeschlagene Schritte in Verfahren *nicht* protokolliert.
- **Protokollierung der erfolgreichen Ausführung von untergeordnetem Script verhindern** – Die Seite "System > **Konfigurieren** *(siehe 429)*" enthält die Option **Protokollieren für erfolgreiche Ausführung von untergeordnetem Script in Agent-Verfahrensprotokoll aktivieren**. Wenn diese Option nicht aktiviert ist, wird die erfolgreiche Ausführung von untergeordneten Scripts nicht in das **Agent-Verfahrensprotokoll** *(siehe 35)* aufgenommen. Damit kann die Größe des Agent-Verfahrensprotokolls drastisch reduziert werden. Es dauert bis zu 5 Minuten, bis der KServer diese Einstellungsänderungen gelesen hat.
- **Ansichtdefinitionen** – Mithilfe der folgenden Optionen für Agent-Verfahren in **Ansichtdefinitionen** *(siehe 27)* können Sie die Anzeige von Rechner-IDs auf jeder Agent-Seite filtern.
  - **Mit geplantem/nicht geplantem Verfahren**
  - **Letzter Ausführungsstatus erfolgreich/fehlgeschlagen**
  - **Verfahren wurde in den letzten N Tagen ausgeführt/nicht ausgeführt**

Aktionsschaltflächen

Agent-Verfahren werden mithilfe von zwei Ordnerstrukturen im mittleren Feld unterhalb der Cabinets **Persönlich** und **Gemeinsam nutzen** organisiert. Je nach ausgewähltem Objekt in der Ordnerstruktur werden folgende Aktionsschaltflächen angezeigt.

Bei Auswahl eines Cabinets

- **Alle ausblenden** – Blendet alle Verzweigungen der Ordnerstruktur aus.
- **Alle erweitern** – Zeigt alle Verzweigungen der Ordnerstruktur an.

Immer verfügbar

- **Dateien verwalten** – Weitere Informationen finden Sie unter **Auf dem Server gespeicherte Dateien verwalten** *(siehe 124)*.
- **Variablen verwalten** – Weitere Informationen finden Sie unter **Variablen-Manager** *(siehe 123)*.

- **(Filter anwenden)** – Geben Sie Text in das Bearbeitungsfeld des Filters ein und klicken Sie dann auf das Trichtersymbol, um das Filtern auf die Ordnerstrukturen anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in den Ordnerstrukturen gefunden wird.

Bei Auswahl eines Ordners

- **Ordner gemeinsam nutzen** – Der Ordner wird mit Benutzerrollen und einzelnen Benutzern freigegeben. *Dies gilt nur für gemeinsam genutzte Cabinetordner.*

> **Hinweis:** Richtlinien für Nutzungsrechte zu Objekten in Ordnerstrukturen finden Sie unter dem Thema **Ordnerrechte** *(siehe 125)*.

- **Neues Verfahren** – Öffnet den Agent-Verfahren-Editor, um ein neues Verfahren im ausgewählten Ordner der Ordnerstruktur zu erstellen. Siehe **Agent-Verfahren erstellen/bearbeiten** *(siehe 95)*.
- **Ordner hinzufügen** – Erstellt einen neuen Ordner unterhalb des ausgewählten Cabinet oder Ordners.
- **Ordner löschen** – Löscht einen ausgewählten Ordner.
- **Ordner umbenennen** – Benennt einen ausgewählten Ordner um.
- **Ordner/Verfahren importieren** – Importiert einen Ordner oder ein Verfahren als untergeordneten Ordner zum ausgewählten Ordner in der Ordnerstruktur. *Gilt nur für private Cabinet-Ordner.*
- **Ordner exportieren** – Exportiert den ausgewählten Ordner und alle seine Verfahren als XML-Datei. Die XML-Datei kann erneut importiert werden.

Zusätzliche Aktionen bei Auswahl eines Verfahrens

- **Verfahren bearbeiten** – Öffnet den Agent-Verfahren-Editor, um das ausgewählte Verfahren zu bearbeiten. Siehe **Agent-Verfahren erstellen/bearbeiten** *(siehe 95)*.
- **Verfahren umbenennen** – Benennt das ausgewählte Verfahren um.
- **Verfahren löschen** – Löscht das ausgewählte Verfahren. Agent-Verfahren, die von anderen Agent-Verfahren verwendet werden, können nicht gelöscht werden.
- **Verfahren exportieren** – Exportiert das ausgewählte Verfahren.

Agent-Verfahren planen

Die Planung von Agent-Verfahren erfolgt über die Registerkarten im rechten Feld. Wenn Sie ein Verfahren im mittleren Feld auswählen, werden im rechten Feld die folgenden Registerkarten angezeigt:

- **Zeitplan** – Wählen Sie eine oder mehrere Rechner-IDs in der Tabelle auf dieser Registerkarte aus und klicken Sie dann auf eine der folgenden Aktionsschaltflächen:
  - **Zeitplanverfahren** – Planen Sie eine einmalige oder periodische Ausführung einer Aufgabe. Jede Art der Wiederholung (einmal, stündlich, täglich, wöchentlich, monatlich, jährlich) zeigt weitere Optionen für diese Art der Wiederholung an. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. *Nicht alle Optionen stehen für jede geplante Aufgabe zur Verfügung.* Optionen können Folgendes umfassen:
    - ✓ **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > **Einstellungen** *(siehe 402)*" festgelegt ist. Übernimmt die Standardeinstellungen aus der Seite "System > **Standardeinstellungen** *(siehe 437)*".
    - ✓ **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die

Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.

- ✓ **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
- ✓ **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
- ✓ **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.

> **Hinweis:** Mit "Agent-Verfahren > **Verteilung** *(siehe 126)*" können Sie die Ausführung von geplanten Agent-Verfahren staffeln.

- ➢ **Jetzt ausführen** – Führen Sie dieses Agent-Verfahren sofort auf jeder ausgewählten Rechner-ID aus.
- ➢ **Abbrechen** – Brechen Sie das geplante Agent-Verfahren auf jeder ausgewählten Rechner-ID ab.

- **Verfahren ansehen** – Liefert eine Nur-Anzeige des Verfahrens. Ein Benutzer kann ein Agent-Verfahren ausführen und anzeigen, ohne es unbedingt bearbeiten zu können. Weitere Informationen finden Sie unter **Ordnerrechte** *(siehe 125)*
- **Verwendet von** – Zeigt eine Liste an, welche anderen Verfahren dieses Verfahren ausführen. Agent-Verfahren, die von anderen Agent-Verfahren verwendet werden, können nicht gelöscht werden.

Agent-Verfahren erstellen/bearbeiten

Agent-Verfahren erstellen/bearbeiten

Um ein neues Verfahren zu erstellen, wählen Sie ein Cabinet oder einen Ordner im mittleren Feld aus und klicken auf die Schaltfläche **Neues Verfahren**. Das Dialogfeld **Agent-Verfahren erstellen/bearbeiten** *(siehe 95)* wird geöffnet.

Um ein vorhandenes Verfahren zu bearbeiten, wählen Sie es aus und klicken auf **Verfahren bearbeiten**. Das Dialogfeld **Agent-Verfahren erstellen/bearbeiten** *(siehe 95)* wird geöffnet. Sie können auch auf ein Verfahren doppelklicken, um es zu bearbeiten.

> **Hinweis:** Ob Sie Verfahren erstellen oder bearbeiten können, hängt von Ihren **Ordnerrechten** *(siehe 125)* ab.

Der Agent-Verfahrenseditor

Alle Anweisungen, die Sie einem Agent-Verfahren hinzufügen können, werden im linken Feld angezeigt. Die Agent-Verfahren werden im mittleren Feld des Editors auf einer oder mehreren der Registerkarten angezeigt. Die Parameter für jede Anweisung werden im rechten Feld angezeigt.

> **Hinweis:** Eine detaillierte Erläuterung der Parameter jeder Anweisung finden Sie unter **IF-THEN-SCHRITT-Befehle** *(siehe 97)*.

Aktionsschaltflächen

Diese Schaltflächen werden im mittleren Feld des Verfahren-Editors angezeigt.

- **Verfahren**
  - ➢ **Neu** – Erstellt eine leere Registerkarte für ein neues Verfahren.

  - **Öffnen** – Bearbeitet ein bestehendes Verfahren.
  - **Speichern** – Speichert das aktuell ausgewählte Verfahren.
  - **Speichern unter** – Speichert das Verfahren unter einem anderen Namen. In einem Dialogfeld können Sie auswählen, in welchem Ordner das Verfahren gespeichert werden soll.
- **Bearbeiten** – Die folgenden Schaltflächen sind nur aktiviert, wenn mindestens eine Anweisung ausgewählt ist.
  - **Rückgängig machen** – Macht die letzte Bearbeitung rückgängig.
  - **Wiederholen** – Wiederholt die letzte Bearbeitung.
  - **Ausschneiden** – Schneidet die ausgewählten Zeilen aus.
  - **Kopieren** – Kopiert die ausgewählten Zeilen.
  - **Einfügen** – Fügt die ausgewählten Zeilen ein.
  - **Entfernen** – Entfernt die ausgewählten Zeilen.
  - **Gehe zu Zeile** – Wählt die angegebene Zeilennummer aus.
  - **Suchen** – Sucht nach übereinstimmenden Text in Befehlen, Parametern und Werten.
  - **Zeile einfügen** – Fügt eine leere Zeile ein, in die Sie Text eingeben können. Dabei wird eine Dropdown-Liste mit Befehlen angezeigt, die Sie auswählen und in das Verfahren einfügen können.
  - **Zeilen einrücken** – Rückt die ausgewählten Zeilen ein.
  - **Zeilen ausrücken** – Rückt die ausgewählten Zeilen aus.
- **Hilfe**
  - **Hilfe-Tipps** – Zeigt Quickinfos zur Verwendung des Verfahren-Editors an.
  - **Online-Hilfe** – Zeigt die Online-Hilfe an.

Drag-and-Drop

- Anweisungen können per Drag-and-Drop über oder unter eine bestehende Anweisung gezogen und dort abgelegt werden.
- Auch Kommentare können über oder unter eine bestehende Anweisung gezogen und abgelegt werden.
- Alle Anweisungen mit Ausnahme von ELSE-Anweisungen werden automatisch eingerückt, wenn sie unterhalb einer IF-Anweisung eingefügt werden.
- Sie können Schritte innerhalb mehrerer IF- oder ELSE-Anweisungen verschachteln. Ziehen Sie einfach eine IF- oder ELSE-Anweisung unter eine IF-Anweisung, um sie automatisch als untergeordnete Anweisung einzufügen.

Richtlinien

- Klicken Sie auf eine Schritt-, IF- oder ELSE-Anweisung im mittleren Feld, um deren Eigenschaften im rechten Feld anzuzeigen. Die Einstellungen können im rechten Feld oder durch Klicken auf einen Wert direkt in der Anweisung geändert werden.
- Sie können mehrere Zeilen gleichzeitig auswählen und bearbeiten.
- Klicken Sie mit der rechten Maustaste auf die ausgewählten Zeilen, um weitere Optionen anzuzeigen.
- Wenn Sie oben im linken Feld einen Wert eingeben, können Sie die Liste der auswählbaren Anweisungen filtern.
- Wenn Sie im linken oder mittleren Feld mit dem Cursor auf eine Anweisung zeigen, sehen Sie eine Quickinfo mit einer Beschreibung der betreffenden Anweisung. Dieselbe Beschreibung wird auch am oberen Rand des dritten Felds angezeigt.
- Wenn Sie mit dem Cursor links neben eine ausgewählte Anweisung zeigen, werden die Symbole angezeigt. Damit können Sie die ausgewählte Anweisung entfernen bzw. ein- oder ausrücken.

- Bei der Eingabe von Werten in einen Parameter haben Sie folgende Möglichkeiten:
  - Geben Sie < ein, um eine Auswahl aus einer Liste von Systemvariablen zu treffen.
  - Geben Sie # ein, um eine Auswahl aus einer Liste von **benutzerdefinierten Variablen** *(siehe 120)* zu treffen.
- Sie können mehrere Verfahren gleichzeitig öffnen und bearbeiten. Dabei wird jedes geöffnete Verfahren auf einer separaten Registerkarte angezeigt. Verfahren können zwischen Registerkarten hin- und herkopiert werden.
- Sie können einen SCHRITT auf `Continue on Fail` setzen. Damit kann ein Verfahren auch dann weiter ausgeführt werden, wenn dieser bestimmte SCHRITT fehlschlägt.
- Klicken Sie auf die leere Zeile am unteren Rand des Verfahrens, um die Beschreibung des gesamten Verfahrens zu bearbeiten.

IF-ELSE-Schritt-Befehle

Es folgt eine Zusammenfassung der IF-ELSE-SCHRITT-Befehle, die im VSA-Agent-Verfahren verwendet werden.

IF-Definitionen

checkVar() *(siehe 101)*	Wertet die angegebene Agent-Variable aus. Siehe **Variablen verwenden** *(siehe 120)*.
else *(siehe 101)*	Fügt einen **ELSE**-Zweig hinzu, um Schritte auszuführen, wenn ein **IF**-Zweig den Wert `False` zurückgibt.
eval() *(siehe 101)*	Vergleicht eine Variable mit einem gelieferten Wert.
getOS() *(siehe 102)*	Bestimmt, ob das aktuelle Windows Betriebssystem 32- oder 64-bit ist.
getRAM() *(siehe 102)*	Überprüft den beim letzten Audit des Agents gemeldeten Gesamtspeicher.
getRegistryValue() *(siehe 102)*	Wertet den angegebenen Registrierungswert aus.
hasRegistryKey() *(siehe 103)*	Testet auf das Vorhandensein des gegebenen Registrierungsschlüssels.
isAppRunning() *(siehe 103)*	Hiermit wird überprüft, ob eine angegebene Anwendung gegenwärtig auf dem verwalteten Rechner ausgeführt wird.
isServiceRunning() *(siehe 103)*	Ermittelt, ob ein Dienst auf dem verwalteten Rechner ausgeführt wird.
isUserActive() *(siehe 103)*	Legt Status des Benutzers fest: • In Ruhestellung oder nicht angemeldet oder • Aktiv
isUserLoggedin() *(siehe 103)*	Testet, ob ein bestimmter Benutzer oder irgendein Benutzer angemeldet ist oder nicht.
isYesFromUser() *(siehe 103)*	Dem Benutzer wird ein Dialogfeld mit **Ja/Nein** angezeigt.
testFile() *(siehe 104)*	Testet auf Vorhandensein einer Datei.
testFileInDirectoryPath() *(siehe 104)*	Prüft den aktuellen Verzeichnispfad, der von **getDirectoryPathFromRegistry()** zurückgegeben wird, auf das Vorhandensein einer Datei.
true *(siehe 104)*	Gibt immer `True` zurück und führt den **IF**-Zweigs aus.

SCHRITT-Definitionen

alarmsSuspend() *(siehe 104)*	Unterdrückt während des angegebenen Zeitraums in Minuten sämtliche Alarme auf einem Rechner.
alarmsUnsuspendAll() *(siehe 104)*	Hebt die Unterdrückung von Alarmen auf einem Rechner auf.

captureDesktopScreenshot() *(siehe 105)*	Erfasst einen Desktop-Screenshot des Agent-Rechners und lädt ihn auf den Kaseya Server hoch.
changeDomainUserGroup() *(siehe 105)*	Ändert die Zugehörigkeit eines Domänenbenutzers in einer Domänenbenutzergruppe.
changeLocalUserGroup() *(siehe 105)*	Ändert die Zugehörigkeit eines lokalen Benutzers in einer lokalen Benutzergruppe.
closeApplication() *(siehe 105)*	Schließt eine laufende Anwendung.
comment() *(siehe 105)*	Fügt dem Verfahren einen einzeiligen Kommentar hinzu.
copyFile() *(siehe 105)*	Kopiert eine Datei von einem Verzeichnis in ein anderes.
copyUseCredentials() *(siehe 105)*	Kopiert eine Datei unter Verwendung von Benutzeranmeldedaten von einem Verzeichnis in ein anderes.
createDomainUser() *(siehe 106)*	Fügt einen neuen Benutzer zu einer Active-Directory-Domäne hinzu, wenn Ausführung auf einem Domänencontroller erfolgt.
createEventLogEntry() *(siehe 106)*	Erstellt einen Ereignisprotokolleintrag bei Anwendungs-, Sicherheits- oder Systemprotokolltypen. Sie können eine Warnung, einen Fehler oder ein Informationsereignis mit Ihrer eigenen Beschreibung erstellen.
createLocalUser() *(siehe 106)*	Fügt einen neuen lokalen Benutzer zu einem Rechner hinzu.
createWindowsFileShare() *(siehe 106)*	Erstellt eine neue Dateifreigabe auf einem Windows Rechner.
deleteDirectory() *(siehe 106)*	Löscht ein Verzeichnis vom Agent-Rechner.
deleteFile() *(siehe 106)*	Löscht eine Datei vom verwalteten Rechner.
deleteFileInDirectoryPath() *(siehe 107)*	Löscht die Datei im Verzeichnis, das von **getDirectoryPathFromRegistry()** zurückgegeben wird.
deleteRegistryKey() *(siehe 107)*	Löscht einen Schlüssel aus der Registrierung.
delete64BitRegistryKey() *(siehe 107)*	Löscht einen**64-bit** *(siehe 119)*-Schlüssel aus der Registrierung.
deleteRegistryValue() *(siehe 107)*	Löscht einen Wert aus der Registrierung.
delete64BitRegistryValue() *(siehe 107)*	Löscht einen **64-bit** *(siehe 119)*-Wert aus der Registrierung.
deleteUser() *(siehe 107)*	Löscht einen Benutzer vom Agent-Rechner.
disableUser() *(siehe 107)*	Deaktiviert einen Benutzer und verhindert die Anmeldung am Agent-Rechner.
disableWindowsService() *(siehe 107)*	Deaktiviert einen Windows Service.
enableUser() *(siehe 107)*	Aktiviert einen zuvor deaktivierten Benutzer und ermöglicht dem Benutzer, sich am Betriebssystem anzumelden.
executeFile() *(siehe 107)*	Führt jede Datei so aus, als ob sie über **Ausführen** im **Windows**-Startmenü ausgeführt würde.
executeFileInDirectoryPath() *(siehe 108)*	Dies entspricht "Datei ausführen". Der Speicherort der Datei ist relativ zum Verzeichnis, das von **getDirectoryPathFromRegistry()** zurückgegeben wird.
executePowershell() *(siehe 108)*	Führt eine/n Powershell-Datei oder -Befehl mit Argumenten aus oder beide.
executePowerShell32BitSystem *(siehe 108)*	Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als 32-Bit-Systembefehl aus.
executePowerShell32BitUser *(siehe 108)*	Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als 32-Bit-Benutzerbefehl aus.
executePowerShell64BitSystem *(siehe 108)*	Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als 64-Bit-Systembefehl aus.
executePowerShell64BitUser *(siehe 108)*	Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als 64-Bit-Benutzerbefehl aus.

executeProcedure() *(siehe 108)*	Startet ein anderes VSA-Agent-Verfahren auf dem aktuellen Rechner.
executeShellCommand() *(siehe 108)*	Führt jeden Befehl aus einer Befehls-Shell aus.
executeShellCommandToVariable() *(siehe 109)*	Führt einen Shellbefehl aus und gibt während und nach der Ausführung erstellte Ergebnisse an eine Variable zurück.
executeVBScript() *(siehe 109)*	Führt ein Vbscript aus, mit oder ohne Befehlszeilenargumente.
getDirectoryPathFromRegistry() *(siehe 109)*	Gibt den Verzeichnispfad aus, der in der Registrierung am angegebenen Speicherort gespeichert ist. Das Ergebnis wird in anschließenden Schritten verwendet.
getFile() *(siehe 109)*	Ruft eine Datei vom verwalteten Rechner ab und speichert sie auf dem Kaseya Server.
getFileInDirectoryPath() *(siehe 110)*	Ruft eine Datei vom verwalteten Rechner ab, dessen Speicherplatz relativ zum von **getDirectoryPathFromRegistry()** zurückgegeben Verzeichnis ist, und speichert sie auf dem Kaseya Server.
getRelativePathFile() *(siehe 110)*	Lädt eine Datei aus einem verwalteten Rechner in einen genehmigten Pfad auf dem Kaseya Server hoch.
getURL() *(siehe 110)*	Gibt den Text und HTML-Inhalt einer URL aus und speichert sie in einer Datei auf dem verwalteten Rechner.
getURLUsePatchFileSource() *(siehe 111)*	Lädt eine Datei von einer vorgegebenen URL in einen Zielordner und Datei für den Agent herunter. Verwendet die Patch-Management >-Datei-Quelleinstellungen.
getVariable() *(siehe 111)*	Ruft einen Wert vom Agent auf dem verwalteten Rechner ab und weist ihn einer Variable zu. Siehe **Variablen verwenden** *(siehe 120)*.
getVariableRandomNumber() *(siehe 111)*	Erzeugt eine Zufallszahl.
getVariableUniversalCreate() *(siehe 111)*	Ruft eine Variable ab, die außerhalb der unmittelbaren Ausführung des Verfahrens weiter besteht.
getVariableUniversalRead() *(siehe 111)*	Liest bis zu drei zuvor mit dem Schritt **getVariableUniversalCreate()** erstellte Variablen.
giveCurrentUserAdminRights() *(siehe 112)*	Fügt den aktuellen Benutzer zur lokalen Administratorgruppe auf dem Agent-Rechner hinzu, entweder dauerhaft oder für eine befristete Zeit.
impersonateUser() *(siehe 112)*	Bestimmt, welches Benutzerkonto bei Ausführung einer Datei oder eines Shell verwendet werden soll, wenn **Als anmeldeter Benutzer ausführen** im nachfolgenden Befehl angegeben ist.
installAptGetPackage() *(siehe 112)*	Installiert ein Paket im Hintergrund über den Befehl `apt-get` in Linux.
installDebPackage() *(siehe 112)*	Installiert ein Debian-Paket im Hintergrund auf jedem Linux-Betriebssystem, das `.deb`-Pakete unterstützt.
installDMG() *(siehe 112)*	Installiert im Hintergrund ein `.DMG`-Paket in OS X.
installMSI() *(siehe 112)*	Installiert eine MSI-Datei für Windows.
installPKG() *(siehe 112)*	Installiert im Hintergrund ein `.PKG`-Paket in OS X.
installRPM() *(siehe 112)*	Installiert im Hintergrund ein RPM-Paket auf jedem Linux Betriebssystem, das die Installation von RPMs unterstützt.
logoffCurrentUser() *(siehe 112)*	Aktueller Benutzer wird automatisch abgemeldet.
pauseProcedure() *(siehe 113)*	Hält das Verfahren für N Sekunden an.
reboot() *(siehe 113)*	Startet den verwalteten Rechner neu.
rebootWithWarning() *(siehe 113)*	Startet einen Rechner neu und zeigt dabei dem zuvor angemeldeten Benutzer eine Warnmeldung an, bevor der Neustart beginnt.
removeWindowsFileShare() *(siehe 113)*	Entfernt eine Dateifreigabe von einem Windows Agent.
renameLockedFile() *(siehe 113)*	Benennt eine Datei um, die gegenwärtig verwendet wird.

renameLockedFileInDirectoryPath() *(siehe 113)*	Benennt eine gegenwärtig verwendete Datei im Verzeichnis um, das von **getDirectoryPathFromRegistry()** zurückgegeben wird.
scheduleProcedure() *(siehe 113)*	Planen Sie ein Agent-Verfahren, das auf einem angegebenen Rechner ausgeführt werden soll.
sendAlert() *(siehe 113)*	Erstellt eine Meldung auf Grundlage eines früheren **getVariable()**-Befehls.
sendEmail() *(siehe 115)*	Sendet eine E-Mail an einen oder mehrere Empfänger.
sendMessage() *(siehe 115)*	Zeigt eine Nachricht in einem Dialogfeld auf dem verwalteten Rechner an.
sendURL() *(siehe 115)*	Öffnet einen Browser an der angegebenen URL auf dem verwalteten Rechner.
setRegistryValue() *(siehe 115)*	Stellt den Registrierungswert auf einen bestimmten Wert ein.
set64BitRegistryValue() *(siehe 115)*	Stellt den **64-bit** *(siehe 119)*-Registrierungswert auf einen bestimmten Wert ein.
sqlRead() *(siehe 116)*	Gibt einen Wert aus einer Datenbank zurück und speichert ihn durch Ausführung eines ausgewählten SQL-"Read"-Befehls in einer umbenannten Variablen.
sqlWrite() *(siehe 116)*	Aktualisiert die Datenbank über einen ausgewählten SQL-"Write"-Befehl.
startWindowsService() *(siehe 117)*	Führt einen Startbefehl für einen Windows Service aus, sofern er existiert.
stopWindowsService() *(siehe 117)*	Führt einen Startbefehl für einen Windows Service aus, sofern er existiert.
transferFile() *(siehe 117)*	Überträgt eine Datei von dem Agent-Rechner, der gerade diesen Schritt ausführt, auf einen anderen Agent-Rechner.
uninstallbyProductGUID() *(siehe 117)*	Deinstalliert im Hintergrund ein Produkt auf Basis seiner MSI-GUID.
unzipFile() *(siehe 117)*	Extrahiert den Inhalt einer bestimmten Zip-Datei in einen Zielordner.
updateSystemInfo() *(siehe 117)*	Aktualisiert das Feld **Systeminformationen** mit den angegebenen Daten.
useCredential() *(siehe 117)*	Gibt an, dass **Anmeldeinformationen einrichten** verwendet werden soll, wenn **Als angemeldeter Benutzer ausführen** in einem nachfolgenden Befehl angegeben ist.
windowsServiceRecoverySettings() *(siehe 118)*	Richtet die Einstellungen für Service-Wiederherstellungen für jeden beliebigen Windows Service ein.
writeDirectory() *(siehe 118)*	Schreibt ein Verzeichnis vom Server auf den verwalteten Rechner.
writeFile() *(siehe 118)*	Schreibt eine auf dem Kaseya Server gespeicherte Datei auf den verwalteten Rechner.
writeFileFromAgent() *(siehe 118)*	Überträgt eine Datei von einem anderen Agent-Rechner auf den Agent-Rechner, der gerade diesen Schritt ausführt.
writeFileInDirectoryPath() *(siehe 119)*	Schreibt eine auf dem Kaseya Server gespeicherte Datei auf den verwalteten Rechner in dem Verzeichnis, das von **getDirectoryPathFromRegistry()** zurückgegeben wird.
writeProcedureLogEntry() *(siehe 119)*	Schreibt eine Zeichenfolge in das Agent-Verfahren-Protokoll.
writeTextToFile() *(siehe 119)*	Schreibt Text in eine Datei auf dem Agent-Rechner.
zipDirectory() *(siehe 119)*	Komprimiert ein Verzeichnis und jegliche Unterverzeichnisse oder Dateien, die es enthält, in eine Zip-Datei auf dem Agent-Rechner.
zipFiles() *(siehe 119)*	Komprimiert eine einzige Datei oder Dateien in eine Zip-Datei auf dem Agent-Rechner.

IF-Befehle

checkVar()

Geben Sie im vorgesehenen Feld einen Variablennamen im Format `#var_name#` ein. **checkVar()** wertet die dem `#var_name#` aktuell zugewiesenen Werte aus und vergleicht sie mit dem gelieferten Wert. Der gelieferte Wert kann auch ein anderer Variablenname im Format `#var_name2#` sein. Falls die Prüfung "wahr" ergibt, werden **WENN**-Befehle ausgeführt. Falls die Prüfung "falsch" ergibt, werden **SONST**-Schritte ausgeführt. Siehe **Variablen verwenden** *(siehe 120)*. Dies sind die verfügbaren Tests:

- `Exists`: wahr, wenn die Variable vorhanden ist
- `Does Not Exist`: wahr, wenn die Variable *nicht* vorhanden ist
- `=`: wahr, wenn der Wert der Variable dem Testwert entspricht
- `Not =`: wahr, wenn der Wert der Variable *nicht* dem Testwert entspricht
- `>`: wahr, wenn der Wert der Variable größer als der Testwert ist
- `>=`: wahr, wenn der Wert der Variable größer/gleich dem Testwert ist
- `<`: wahr, wenn der Wert der Variable kleiner als der Testwert ist
- `<=`: wahr, wenn der Wert der Variable kleiner/gleich dem Testwert ist
- `Contains`: wahr, wenn der Testwert eine untergeordnete Zeichenfolge des Variablenwerts ist
- `Not Contains`: wahr, wenn der Testwert *keine* untergeordnete Zeichenfolge des Variablenwerts ist
- `Begins With`: wahr, wenn der Variablenwert mit dem Testwert beginnt
- `Ends With`: wahr, wenn der Variablenwert mit dem Testwert endet

Bei den Tests `=`, `Not =`, `>`, `>=`, `<` und `<=` können die verglichenen Variablen eine Zeichenfolge, eine Zahl, ein Datum im Format `yyyy/mm/dd` oder `yyyy/mm/dd hh:mm` bzw. `yyyy/mm/dd hh:mm:ss` oder eine Versionsnummer sein, die Punkte oder Kommas enthält, etwa `1.2.3` oder `4,5,6,7`. Werte in Variablen werden als Zeichenfolgen gespeichert; verglichene Zahlen müssen also dieselbe Zeichenfolgenlänge aufweisen. Wenn ein Datumsformat angegeben wird, kann es durch Eingabe von `+ dd:hh:mm:ss` oder `- dd:hh:mm:ss` versetzt werden. Nur `dd` (Tage) sind erforderlich; `hh` (Stunden), `mm` (Minuten) und `ss` (Sekunden) können ausgelassen werden. In diesem Fall werden sie als null betrachtet. `CURRENT_TIMESTAMP` kann angegeben werden, um anzudeuten, dass die aktuelle Uhrzeit im Vergleich zum Zeitpunkt der Verfahrensausführung ersetzt werden soll: `CURRENT_TIMESTAMP - 7:12:00:00` wird z. B. als 7 Tage und 12 Stunden, subtrahiert von der Uhrzeit der Verfahrensausführung, ausgewertet.

else

Fügt unterhalb des entsprechenden **IF**-Befehls einen **ELSE**-Befehl ein. Alle Schritte im **ELSE**-Befehl werden ausgeführt, wenn der betreffende **IF**-Befehl `False` zurückgibt.

eval()

Geben Sie im vorgesehenen Feld einen oder mehrere Variablennamen im Format `#var_name#` ein. **checkVar()** zieht den aktuell jedem `#var_name#` zugewiesenen Wert heran, wertet den mathematischen Ausdruck aus und vergleicht ihn mit dem gelieferten Wert. Der gelieferte Wert kann auch ein anderer Ausdruck sein. Der mathematische Ausdruck kann `+`, `-`, `*`, `/`, `(` und `)` enthalten. Beispiel: `(3.7 + (200 * #countA#)) / (#countB# - #countC#)`. Wenn die IF-Prüfung

wahr ergibt, werden die **IF**-Schritte ausgeführt. Falls die Prüfung "falsch" ergibt, werden **SONST**-Schritte ausgeführt. Dies sind die verfügbaren Tests:

- `=`: wahr, wenn der Wert der Variable dem Testwert entspricht
- `Not =`: wahr, wenn der Wert der Variable nicht dem Testwert entspricht
- `>`: wahr, wenn der Wert der Variable größer als der Testwert ist
- `>=`: wahr, wenn der Wert der Variable größer/gleich dem Testwert ist
- `<`: wahr, wenn der Wert der Variable kleiner als der Testwert ist
- `<=`: wahr, wenn der Wert der Variable kleiner/gleich dem Testwert ist

> **Hinweis:** Kann nicht mit den Operatoren `Exists`, `Does Not Exist`, `Contains` oder `Not Contains` verwendet werden.

getOS()

Bestimmt, ob das aktuelle Windows Betriebssystem 32- oder 64-bit ist.

Unterstützte Betriebssysteme: Windows

getRAM()

Überprüft den beim letzten Audit des Agents gemeldeten Gesamtspeicher. Das kann nützlich sein, wenn Sie sicherstellen wollen, dass ein System die Voraussetzungen für eine Anwendung erfüllt, bevor die Installation begonnen wird.

Unterstützte Betriebssysteme: Windows, OS X, Linux

getRegistryValue() / get64BitRegistryValue() *(siehe 119)*

Nach Eingabe des Registrierungspfads wird der im Schlüssel enthaltene Wert ausgegeben. Es kann auf Vorhandensein, Nichtvorhandensein, Gleichheit oder Größenunterschiede überprüft werden. `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\AppPaths\AgentMon.exe\path` enthält zum Beispiel den Verzeichnispfad, der angibt, wo der Agent auf dem Zielrechner installiert ist. Der Test ermittelt, ob der für diesen Schlüssel gespeicherte Wert vorhanden ist und überprüft auf diese Weise, ob der Agent installiert ist.

Dies sind die verfügbaren Tests:

- `Exists`: wahr, wenn der Registrierungsschlüssel im Hive existiert
- `Does Not Exist`: wahr, wenn der Registrierungsschlüssel im Hive *nicht* existiert
- `=`: wahr, wenn der Wert des Registrierungsschlüssels dem Testwert entspricht
- `Not =`: wahr, wenn der Wert des Registrierungsschlüssels dem Testwert *nicht* entspricht
- `>`: wahr, wenn der Wert des Registrierungsschlüssels größer als der Testwert ist (der Wert muss eine Zahl sein)
- `>=`: wahr, wenn der Wert des Registrierungsschlüssels größer/gleich dem Testwert ist (der Wert muss eine Zahl sein)
- `<`: wahr, wenn der Wert des Registrierungsschlüssels kleiner als der Testwert ist (der Wert muss eine Zahl sein)
- `<=`: wahr, wenn der Wert des Registrierungsschlüssels kleiner/gleich Testwert ist (der Wert muss eine Zahl sein)
- `Contains`: wahr, wenn der Testwert eine untergeordnete Zeichenfolge des Registrierungsschlüsselwerts ist (der Wert muss eine Zeichenfolge sein)
- `Not Contains`: wahr, wenn der Testwert *keine* untergeordnete Zeichenfolge des Registrierungsschlüsselwerts ist (der Wert muss eine Zeichenfolge sein)

Verwendung des umgekehrten Schrägstrichs (\)

Ein umgekehrter Schrägstrich `\` am Ende des Schlüssels gibt den Standardwert dieses Schlüssels

zurück. `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WORDPAD.EXE\` gibt einen Standardwert zurück, etwa `%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE`

Der *letzte einzelne Schrägstrich* in einer Zeichenfolge dient zur Abgrenzung des Registrierungsschlüssels vom Registrierungswert. Wenn Ihre Zeichenfolge Schrägstriche enthalten soll, müssen diese als *doppelte Schrägstriche* angegeben werden. Die Zeichenfolge `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Value\\Name` wird beispielsweise als Schlüssel namens `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey` mit dem Wert `Value\Name` interpretiert.

hasRegistryKey()/has64bitRegisterKey() *(siehe 119)*

Prüft auf Vorhandensein eines Registrierungsschlüssels. **hasRegistryKey()** unterscheidet sich von **getRegistryValue()**, da es auf einen Registrierungseintrag auf Verzeichnisebene prüfen kann, der nur weitere Registrierungsschlüssel (und keine Werte) enthält.

isAppRunning()

Hiermit wird überprüft, ob eine angegebene Anwendung gegenwärtig auf dem verwalteten Rechner ausgeführt wird. Ist dies der Fall, wird der **FALLS**-Befehl ausgeführt. Wenn nicht, wird der **SONST**-Befehl ausgeführt. Bei Auswahl dieser Option aus der Dropdown-Liste wird das Feld **Anwendungsnamen eingeben** angezeigt. Geben Sie den Verfahrensnamen für die Anwendung an, die getestet werden soll. Wenn Sie zum Beispiel die Anwendung `Calculator` testen möchten, geben Sie `calc.exe` an. Dies ist der Prozessname, der auf der Registerkarte **Prozesse** im **Task-Manager** in Windows angezeigt wird.

isServiceRunning()

Ermittelt, ob ein Dienst auf dem verwalteten Rechner ausgeführt wird. Geben Sie den *Dienstnamen* an.

- Wahr, falls der Dienstname ausgeführt wird.
- Falsch, falls der Dienstname angehalten wurde oder nicht vorhanden ist.

> **Hinweis:** Achten Sie darauf, den *Dienstnamen* des Dienstes und nicht seinen *Anzeigenamen* zu verwenden. Der *Anzeigename* des Dienstes für Microsoft SQL Server ist beispielsweise `SQL Server (MSSQLSERVER)`, aber sein *Dienstname* ist `MSSQLSERVER`. Bei Windows-Rechnern klicken Sie im Fenster **Dienste** mit der rechten Maustaste auf einen beliebigen Dienst und klicken dann auf die Option **Eigenschaften**, um den *Dienstnamen* dieses Dienstes anzuzeigen.

isUserActive()

Legt Status des Benutzers fest:

- In Ruhestellung oder nicht angemeldet oder
- Aktiv

Unterstützte Betriebssysteme: Windows, OS X, Linux

isUserLoggedin()

Testet, ob ein bestimmter Benutzer oder ein beliebiger Benutzer am verwalteten Rechner angemeldet ist. Geben Sie den Anmeldenamen des Rechnerbenutzers ein oder lassen Sie das Feld leer, um zu überprüfen, ob irgendein Benutzer angemeldet ist. Die **WENN**-Befehle werden ausgeführt, falls ein Benutzer angemeldet ist. Die **SONST**-Befehle werden ausgeführt, falls kein Benutzer angemeldet ist.

isYesFromUser()

Zeigt ein Dialogfeld mit den Schaltflächen **Ja** und **Nein** auf dem verwalteten Rechner an. Es führt außerdem den **SONST**-Befehl aus, falls ein festgelegter Zeitraum verstrichen ist. Wenn **Ja** vom

Rechnerbenutzer ausgewählt wird, wird der **WENN**-Befehl ausgeführt. Wenn eine Zeitüberschreitung der Auswahl eintritt oder der Rechnerbenutzer **Nein** auswählt, wird der **SONST**-Befehl ausgeführt. Diese Funktion fragt um die Erlaubnis des Rechnerbenutzers, mit dem Agent-Verfahren fortzufahren. Diese Anfrage ist nützlich bei Agent-Verfahren, die vor dem Abschluss des Verfahrens einen Neustart des verwalteten Rechners erfordern.

In den Feldern **isYesFromUser()** können Verfahrensvariablen wie `#varName#` verwendet werden, um dynamisch Meldungen zu erzeugen, die auf Verfahrensdaten beruhen.

testFile()

Ermittelt, ob eine Datei auf einem verwalteten Rechner vorhanden ist. Geben Sie den vollständigen Pfad- und Dateinamen ein. **testFile()** vergleicht den vollständigen Pfad- und Dateinamen mit dem gelieferten Wert. Falls die Prüfung "wahr" ergibt, werden **WENN**-Befehle ausgeführt. Falls die Prüfung "falsch" ergibt, werden **SONST**-Schritte ausgeführt.

Hinweis: Umgebungsvariablen wie `%windir%\notepad.exe` sind zulässig.

Dies sind die verfügbaren Tests:

- `Exists`: wahr, wenn der vollständige Pfad- und Dateiname existieren
- `Does not Exist`: wahr, wenn der vollständige Pfad- und Dateiname *nicht* existieren
- `Contains`: wahr, wenn der Testwert eine untergeordnete Zeichenfolge des Dateiinhalts ist
- `Not Contains`: wahr, wenn der Testwert *keine* untergeordnete Zeichenfolge des Dateiinhalts ist
- `Begins With`: wahr, wenn der Testwert mit dem Variablenwert beginnt
- `Ends With`: wahr, wenn der Testwert mit dem Variablenwert endet

testFileInDirectoryPath()

Testet die angegebene Datei am ausgegebenen Pfad mithilfe des Schritts **getDirectoryPathFromRegistry()**. Dies sind die verfügbaren Tests:

- `Exists`: wahr, wenn der Dateiname existiert
- `Does not Exist`: wahr, wenn der Dateiname *nicht* existiert
- `Contains`: wahr, wenn der Testwert eine untergeordnete Zeichenfolge des Dateiinhalts ist
- `Not Contains`: wahr, wenn der Testwert *keine* untergeordnete Zeichenfolge des Dateiinhalts ist
- `Begins With`: wahr, wenn der Testwert mit dem Variablenwert beginnt
- `Ends With`: wahr, wenn der Testwert mit dem Variablenwert endet

true

Bei Auswahl von `True` werden die **IF**-Befehle ausgeführt. Mit **True** können Sie eine Reihe von Schritten direkt ausführen, die keine Entscheidungen benötigen, wie zum Beispiel das Ermitteln des Vorhandenseins einer Datei unter Verwendung von **testFile()**.

SCHRITT-Befehle

alarmsSuspend()

Unterdrückt während des angegebenen Zeitraums in Minuten sämtliche Alarme auf einem Rechner. Aktualisiert den Status von Rechnern auf der Seite "Monitor > Status > **Alarm unterbrechen** *(siehe 262)*".

alarmsUnsuspendAll()

Hebt die Unterdrückung von Alarmen auf einem Rechner auf. Aktualisiert den Status von Rechnern auf der Seite "Monitor > Status > **Alarm unterbrechen** *(siehe 262)*".

captureDesktopScreenshot()

Erfasst einen Desktop-Screenshot des Agent-Rechners und lädt ihn auf den Kaseya Server hoch. Der Screenshot wird unter einem eindeutigen Namen in einem dem Agent fest zugeordneten Ordner als PNG-Datei gespeichert. Sie können auf diese Datei über die Seite "Audit > **Dokumente** *(siehe 158)*" oder über **Live-Connect** *(siehe 393)* zugreifen. Optionen für Endbenutzer-Benachrichtungen können nach Bedarf ausgewählt werden, z.B. Erfassung eines Screenshots im Hintergrund oder die vorherige Benachrichtigung, dass ein Screenshot genommen werden wird oder eine Aufforderung, den Screenshot zu bestätigen. Eine kundespezifische Meldung kann bei den Optionen Benutzerbenachrichtigung oder vorherige Bestätigung durch Benutzer eingegeben werden. Ansonsten wird eine Standardmitteilung angezeigt.

Unterstützte Betriebssysteme: Windows, OS X, Linux

changeDomainUserGroup()

Ändert die Zugehörigkeit eines Domänenbenutzers in einer Domänenbenutzergruppe. Dieser **SCHRITT** muss auf einem Domänencontroller ausgeführt werden. Geben Sie den Domänenbenutzernamen des Mitglieds ein, der zu der Domänenbenutzergruppe hinzugefügt oder von ihr entfernt wurde. Wählen Sie dann, ob Zugehörigkeit hinzugefügt oder entfernt werden soll. Wählen Sie dann die Domänenbenutzergruppe.

Unterstützte Betriebssysteme: Windows

changeLocalUserGroup()

Ändert die Zugehörigkeit eines lokalen Benutzers in einer lokalen Benutzergruppe. Geben Sie den Domänenbenutzernamen des Mitglieds ein, der zu der lokalen Bbenutzergruppe hinzugefügt oder von ihr entfernt wurde. Wählen Sie dann, ob Zugehörigkeit hinzugefügt oder entfernt werden soll. Wählen Sie dann die Gruppe aus.

Unterstützte Betriebssysteme: Windows

closeApplication()

Wenn die angegebene Anwendung auf dem verwalteten Rechner ausgeführt wird, wird sie geschlossen. Geben Sie den Verfahrensnamen für die Anwendung an, die geschlossen werden soll. Wenn Sie zum Beispiel die Anwendung `Calculator` schließen möchten, geben Sie `calc.exe` an. Dies ist der Prozessname, der auf der Registerkarte **Prozesse** im **Task-Manager** in Windows angezeigt wird.

comment()

Fügt dem Verfahren einen einzeiligen Kommentar hinzu.

copyFile()

Kopiert eine Datei auf dem Agent-Rechner von einem Verzeichnis in ein anderes. Wenn die Zieldatei schon vorhanden ist, müssen Sie ein Kontrollkästchen aktivieren, damit die Datei überschrieben werden kann. Achten Sie auf die Ordnersyntax, wenn Sie diesen **SCHRITT** in unterschiedlichen Betriebssystemen durchführen, z. B. `c:\temp\tempfile.txt` für Windows und `/tmp/tempfile.txt` für OS X und Linux.

Unterstützte Betriebssysteme: Windows, OS X, Linux

copyUseCredentials()

Kopiert eine Datei aus einem Verzeichnis auf einen Rechner und versucht die Datei in eine Ziellaufwerk und Dateinamen zu kopieren. Der Kopierprozess verwendet:

- Die Benutzeranmeldedaten, die für einen Agent über Agent > **Anmeldedaten einrrichten** *(siehe 77)* festgelegt wurden oder
- Die Benutzeranmeldedaten, die über den Schritt **impersonateUser()** vorher festgelegt wurden.

Dieser **SCHRITT** wird hauptsächlich zum Zugriff auf Dateien über UNC-Netzwerkfreigaben verwendet. Wenn die Zieldatei schon vorhanden ist, müssen Sie ein Kontrollkästchen aktivieren, damit die Datei überschrieben werden kann. Achten Sie auf die Ordnersyntax, wenn Sie diesen **SCHRITT** in unterschiedlichen Betriebssystemen durchführen, z. B. `c:\temp\tempfile.txt` für Windows und `/tmp/tempfile.txt` für OS X und Linux.

Unterstützte Betriebssysteme: Windows, OS X, Linux

createDomainUser()

Fügt einen neuen Benutzer zu einer Active-Directory-Domäne hinzu, wenn Ausführung auf einem Domänencontroller erfolgt. Geben Sie den Domänenbenutzernamen ein, den Sie erstellen möchten, und ein Kennwort, das die Komplexitätsanforderungen der Domäne für Benutzerkonten erfüllt. Dann wählen Sie die Domänengruppe, der der Benutzer hinzugefügt werden soll, entweder `Domain Users` oder `Domain Admins`.

Unterstützte Betriebssysteme: Windows

createEventLogEntry()

Erstellt einen Ereignisprotokolleintrag bei Anwendungs-, Sicherheits- oder Systemprotokolltypen. Sie können eine Warnung, einen Fehler oder ein Informationsereignis mit Ihrer eigenen Beschreibung erstellen. Das erstellte Ereignis ist hartkodiert auf die Ereignis-ID 607.

Unterstützte Betriebssysteme: Windows

createLocalUser()

Fügt einen neuen lokalen Benutzer zu einem Rechner hinzu. Geben Sie einen lokalen Benutzernamen ein, den Sie erstellen wollen, und ein Kennwort, das die lokalen Komplexitätsanforderungen für Benutzerkonten erfüllt. Dann wählen Sie die Gruppe, der der Benutzer hinzugefügt werden soll.

Unterstützte Betriebssysteme: Windows, OS X, Linux

createWindowsFileShare()

Erstellt eine neue Dateifreigabe auf einem Windows Rechner. Sie müssen den Namen der Dateifreigabe eingeben, da der Zugriff über das Netzwerk erfolgt. Dann geben Sie den Quellordner des Agents für die Dateifreigabe ein. Dieser Ordner wird erstellt, wenn er noch nicht vorhanden ist.

Unterstützte Betriebssysteme: Windows

deleteDirectory()

Löscht ein Verzeichnis vom Agent-Rechner. Stellen Sie sicher, dass Sie die korrekte Verzeichnissyntys für Windows vs. OS X/ Linux haben. Um sicherzustellen, dass alle Unterverzeichnisse und Dateien ebenfalls gelöscht wurden, aktivieren Sie das Kontrollkästchen **Unterverzeichnisse und Dateien rekursiv löschen**.

Unterstützte Betriebssysteme: Windows, OS X, Linux

deleteFile()

Löscht eine Datei auf dem verwalteten Rechner. Geben Sie den vollständigen Pfad und Dateinamen ein.

> **Hinweis:** Umgebungsvariablen sind zulässig, wenn sie auf dem Rechner eines Benutzers eingestellt sind. Zum Beispiel ähnelt die Verwendung des Pfads `%windir%\notepad.exe` dem Pfad `C:\windows\notepad.exe`.
>
> **Hinweis:** Mithilfe des Befehls **renameLockedFile()** können Sie eine Datei löschen, die gegenwärtig verwendet wird.

deleteFileInDirectoryPath()

Löscht die angegebene Datei im zurückgegebenen Pfad mithilfe des Befehls **getDirectoryPathFromRegistry()**.

deleteRegistryKey()/delete64BitRegistryKey() *(siehe 119)*

Löscht den angegebenen Registrierungsschlüssel und alle seine Unterschlüssel.

deleteRegistryValue()/delete64BitRegistryValue() *(siehe 119)*

Löscht den Wert, der am angegebenen Registrierungsschlüssel gespeichert ist. Der *letzte einzelne Schrägstrich* in einer Zeichenfolge dient zur Abgrenzung des Registrierungsschlüssels vom Registrierungswert. Wenn Ihre Zeichenfolge Schrägstriche enthalten soll, müssen diese als *doppelte Schrägstriche* angegeben werden. Die Zeichenfolge `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Value\\Name` wird beispielsweise als Schlüssel namens `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey` mit dem Wert `Value\Name` interpretiert.

deleteUser()

Löscht einen Benutzer vom Agent-Rechner.

Unterstützte Betriebssysteme: Windows, OS X, Linux

disableUser()

Deaktiviert einen Benutzer und verhindert die Anmeldung am Agent-Rechner.

Unterstützte Betriebssysteme: Windows, OS X, Linux

disableWindowsService()

Deaktiviert einen Windows Service.

Unterstützte Betriebssysteme: Windows

enableUser()

Aktiviert einen zuvor deaktivierten Benutzer und ermöglicht dem Benutzer, sich am Betriebssystem anzumelden.

Unterstützte Betriebssysteme: Windows, OS X, Linux

executeFile()

Führt die angegebene Datei auf dem verwalteten Rechner aus. Diese Funktion repliziert den Start einer Anwendung mithilfe des Befehls **Ausführen...** im **Startmenü** von Microsoft Windows. Diese Funktion braucht drei Parameter:

- Vollständiger Pfad und Dateiname der `.exe`-Datei
- Argumentliste zum Übergeben an die `.exe`-Datei
- Option zum Aufschub des Verfahrens, bis die `.exe`-Datei abgeschlossen ist oder nicht

> **Hinweis:** Umgebungsvariablen sind zulässig, wenn sie auf dem Rechner eines Benutzers eingestellt sind. Zum Beispiel ähnelt die Verwendung des Pfads `%windir%\notepad.exe` dem Pfad `C:\windows\notepad.exe`.

Falls **Als angemeldeten Benutzer ausführen** ausgewählt ist, müssen vor der Ausführung dieses Befehls Anmeldedaten angegeben werden, und zwar entweder über **impersonateUser()** *(siehe 112)* oder **useCredential()** *(siehe 117)*. Bei Auswahl von **Als Systemkonto ausführen** ist die Ausführung auf die Systemebene des Agent beschränkt.

executeFileInDirectoryPath()

Dies ist mit **Datei ausführen** identisch, außer dass sich der Speicherort der EXE-Datei im vom **getDirectoryPathFromRegistry()** zurückgegebenen Pfad befindet.

Falls **Als angemeldeten Benutzer ausführen** ausgewählt ist, müssen vor der Ausführung dieses Befehls Anmeldedaten angegeben werden, und zwar entweder über **impersonateUser()** *(siehe 112)* oder **useCredential()** *(siehe 117)*. Bei Auswahl von **Als Systemkonto ausführen** ist die Ausführung auf die Systemebene des Agent beschränkt.

executePowershell()

Führt ein Powershell-Skript aus, zusammen mit:

- einer Powershell-`.PS1`-Datei
- einem Powershell-Befehl mit bestimmten Argumenten
- beide zusammen

Unterstützte Betriebssysteme: Windows XP SP3+/Server 2008 mit Powershell Zusatzmodul, Windows 7, Windows Server 2008

Dieser Befehl hat *fünf Varianten*.

- **executePowershell()** – Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides aus. Bei Ausführung dieses Befehls auf einem 32-Bit- oder 64-Bit-Rechner werden keine system- oder benutzerdefinierten Anmeldedaten bereitgestellt.
- **executePowerShell32BitSystem** – Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als *32-Bit-Systembefehl* aus.
- **executePowerShell32BitUser** – Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als *32-Bit-Benutzerbefehl* aus.
- **executePowerShell64BitSystem** – Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als *64-Bit-Systembefehl* aus.
- **executePowerShell64BitUser** – Führt eine Powershell-Datei, einen Powershell-Befehl mit Argumenten oder beides als *64-Bit-Benutzerbefehl* aus.

System- und Benutzerbefehle:

- **System** – Bei Ausführung eines *Systembefehls* ist die Ausführung auf die Systemebene des Agent beschränkt.
- **Benutzer** – Bei Auswahl eines *Benutzerbefehls* müssen vor der Ausführung dieses Befehls Anmeldedaten angegeben werden, und zwar entweder über **impersonateUser()** *(siehe 112)* oder **useCredential()** *(siehe 117)*.

executeProcedure()

Verursacht, dass ein anderes benanntes Verfahren ausgeführt wird. Verwenden Sie diese Funktion, um mehrere **WENN-SONST-SCHRITT**-Verfahren zu verketten. Falls das Verfahren nicht mehr auf dem Kaseya Server vorhanden ist, wird neben der Dropdown-Liste für das Verfahren eine Fehlermeldung angezeigt. Mithilfe dieses Befehls können Sie ein **Systemverfahren** *(siehe 631)* ausführen. Sie können Verfahren auf 10 Ebenen verschachteln.

executeShellCommand()

Dieser Befehl lässt das Verfahren Befehle an den Befehlsübersetzer auf dem verwalteten Rechner übertragen. Bei Auswahl dieses Befehls wird das Feld **Geben Sie den auszuführenden Befehl in eine Befehls-Shell ein** angezeigt. Geben Sie einen Befehl in das Feld ein. Der Befehl muss syntaktisch korrekt und mit der Betriebssystemversion auf dem verwalteten Rechner ausführbar sein. *Befehle und Parameter, die Leerstellen enthalten, sollten in Anführungszeichen eingeschlossen werden.* Da der Befehl relativ zum Agent-Verzeichnis ausgeführt wird, sollten bei der Eingabe von Befehlen absolute Pfade verwendet werden.

> **Hinweis: executeShellCommand()** öffnet eine Befehlszeilenaufforderung auf einem verwalteten Windows-Rechner, in der der Befehl ausgeführt werden kann. Wenn Sie dies nicht wünschen, weil es die Benutzer verwirren könnte, legen Sie alle Befehle in einer Stapeldatei ab. Senden Sie diese Datei über den Befehl **writeFile()** an den verwalteten Rechner. Führen Sie die Stapeldatei dann mit dem Befehl **executeFile()** aus. **executeFile()** öffnet keine Befehlszeilenaufforderung auf verwalteten Windows-Rechnern.

Falls **Als angemeldeten Benutzer ausführen** ausgewählt ist, müssen vor der Ausführung dieses Befehls Anmeldedaten angegeben werden, und zwar entweder über **impersonateUser()** *(siehe 112)* oder **useCredential()** *(siehe 117)*. Bei Auswahl von **Als Systemkonto ausführen** ist die Ausführung auf die Systemebene des Agent beschränkt.

executeShellCommandToVariable()

Führt einen Shellbefehl aus und gibt während und nach der Ausführung erstellte Ergebnisse an eine Variable zurück. Diese Variable muss in nachfolgenden Schritten als `#global:cmdresults#` referenziert werden.

Unterstützte Betriebssysteme: Windows, OS X, Linux

executeVBScript()

Führt ein Vbscript aus, mit oder ohne Befehlszeilenargumente. IfWenn das Vbscript ein Popup-Fenster anzeigt oder den Endbenutzer benachrichtigt, aktivieren Sie das Kontrollkästchen für **Wscript anstelle von Cscript verwenden**.

Unterstützte Betriebssysteme: Windows

getDirectoryPathFromRegistry()

Gibt einen Dateipfad aus, der im angegebenen Registrierungsschlüssel gespeichert ist. Verwenden Sie diesen Befehl, um den Speicherort der Datei abzurufen. So können Sie zum Beispiel das Verzeichnis finden, in dem eine Anwendung installiert wurde. Das Ergebnis kann in nachfolgenden Schritten von Folgendem verwendet werden:

- **deleteFileInDirectoryPath()**
- **executeFileInDirectoryPath()**
- **getFileInDirectoryPath()**
- **renameLockedFileInDirectoryPath()**
- **testFileInDirectoryPath()** (IF-Befehl)
- **writeFileInDirectoryPath()**

getFile()

Laden Sie die Datei am angegebenen Pfad vom verwalteten Rechner hoch. Achten Sie darauf, den vollständigen Pfadnamen der hochzuladenden Datei einzugeben. Beispiel: `news\info.txt`. Bei Ausführung des Befehls **getFile()** werden Ordner erstellt, falls sie noch nicht vorhanden sind. Die Datei wird auf dem Kaseya Server in einem privaten Verzeichnis für jeden verwalteten Rechner gespeichert. Verwenden Sie "Agent-Verfahren > **Datei abrufen** *(siehe 134)*", um die hochgeladene Datei anzuzeigen oder auszuführen.

- Vorhandene Kopien von hochgeladenen Dateien werden optional vor dem nächsten Hochladen der Datei mit einer Erweiterung `.bak` umbenannt. Auf diese Weise können Sie die neueste Version und die ältere Version der Datei untersuchen.
- Erstellen Sie optional die Meldung **Datei abrufen**, falls sich die hochgeladene Datei von der bereits hochgeladenen Datei *unterscheidet* oder mit ihr *identisch* ist. *Sie müssen eine Meldung "Datei abrufen" für eine Rechner-ID* mithilfe der Seite "Monitor > **Meldungen – Datei abrufen** *(siehe 292)*2 erstellen, damit das Senden der Meldung über den Befehl **getFile()** möglich ist. Sobald eine Meldung für eine Rechner-ID definiert wurde, ist dieselbe Meldung **Datei abrufen** für *jedes*

Agent-Verfahren aktiv, das einen Befehl **getFile()** verwendet und auf dieser Rechner-ID ausgeführt wird. Deaktivieren Sie Meldungen für bestimmte Dateien im Agent-Verfahren-Editor, indem Sie eine der Optionen für "Ohne Meldung" auswählen.

getFileInDirectoryPath()

Dies funktioniert genau wie der Befehl **getFile()**, fügt jedoch den vom Befehl **getDirectoryPathFromRegistry()** zurückgegebenen Pfad am Anfang des Remote-Dateipfads hinzu. Der Zugriff auf die hochgeladene Datei erfolgt über die Funktion "Agent-Verfahren > **getFile()** *(siehe 134)*".

getRelativePathFile()

Lädt eine Datei aus einem verwalteten Rechner in einen genehmigten Pfad auf dem Kaseya Server hoch. Der Speicherort der Datei ist relativ zum Verzeichnis `<KaseyaInstallationDirectory>\UserProfiles\<agent guid>\GetFiles`. Die Datei wird auf dem Kaseya Server in einem privaten Verzeichnis für jeden verwalteten Rechner gespeichert. Verwenden Sie "Agent-Verfahren > **Datei abrufen** *(siehe 134)*", um die hochgeladene Datei anzuzeigen oder auszuführen.

- Vorhandene Kopien von hochgeladenen Dateien werden optional vor dem nächsten Hochladen der Datei mit einer Erweiterung `.bak` umbenannt. Auf diese Weise können Sie die neueste Version und die ältere Version der Datei untersuchen.
- Erstellen Sie optional die Meldung **Datei abrufen**, falls sich die hochgeladene Datei von der bereits hochgeladenen Datei *unterscheidet* oder mit ihr *identisch* ist. *Sie müssen eine Meldung "Datei abrufen" für eine Rechner-ID* mithilfe der Seite "Monitor > **Meldungen – Datei abrufen** *(siehe 292)*" erstellen, damit das Senden der Meldung über den Befehl **getRelativePathFile()** möglich ist. Sobald eine Meldung für eine Rechner-ID definiert wurde, ist dieselbe Meldung **Datei abrufen** für *jedes Agent-Verfahren aktiv*, das **getFile()** oder **getRelativePathFile()** verwendet und auf dieser Rechner-ID ausgeführt wird. Deaktivieren Sie Meldungen für bestimmte Dateien im Agent-Verfahren-Editor, indem Sie eine der Optionen für "Ohne Meldung" auswählen.

Die Liste der genehmigten relativen Pfade wird über eine oder mehrere der unter `<KaseyaInstallationDirectory>\xml\Procedures\AgentProcPaths\<partitionId>\getRelativePathFile` vorhandenen XML-Dateien definiert.

Dateinamen können beliebige Namen mit der Erweiterung `.xml` sein, vorausgesetzt, sie sind intern korrekt formatiert. Wenn durch eine oder mehrere XML-Datei(en) mehrere Anweisungen definiert werden, werden diese in der Benutzeroberfläche in einer gemeinsamen Kombinationsfeldliste angezeigt. Jede Anweisung zu einem genehmigten Pfad in der XML-Datei weist eine eigene Bezeichnung auf; nur die Bezeichnungen werden im Kombinationsfeld angezeigt. Wenn keine Anweisungen zu genehmigten Pfaden definiert sind, wird im Kombinationsfeld der Eintrag `*No Approved Paths*` angezeigt.

Partitionsspezifische Anweisungen

Partitionsspezifische Ordner können partitionsspezifische Anweisungen zu genehmigten Pfaden enthalten. Zum Beispiel: `<KaseyaInstallationDirectory>\xml\Procedures\AgentProcPaths\1234567890\getRelativePathFile`. Benutzer können alle Anweisungen zu genehmigten Pfaden im Ordner `0` und im eigenen Partitionspfad auswählen und ausführen.

Beispielformat

```
<pathList>
  <pathDef label="Documents Folder" path="..\Documents"/>
  <pathDef label="Miscellaneous Folder" path="..\Miscellaneous"/>
</pathList>
```

getURL()

Gibt den Text und HTML-Inhalt einer URL aus und speichert sie in einer Datei auf dem verwalteten

Rechner. Probieren Sie Folgendes: Geben Sie `www.kaseya.com` als URL an und `c:\temp\test.htm` als die Datei, in der der Inhalt dieser URL gespeichert werden soll. Auf dem verwalteten Rechner wird eine Kopie der Webseite erstellt, die den gesamten Text und HTML-Inhalt dieser Webseite enthält. Sie können den Inhalt der Datei auf dem verwalteten Rechner mit einem nachfolgenden Befehl durchsuchen.

Eine weitere Verwendung besteht darin, eine ausführbare Datei herunterzuladen, die auf einem Webserver zur Verfügung steht. Dann brauchen Sie die Datei weder auf den VSA-Server hochzuladen noch die VSA-Bandbreite zu verwenden, um die Datei an jeden Agent zu übertragen. Mithilfe eines nachfolgenden Befehls können Sie die heruntergeladene ausführbare Datei auf dem verwalteten Rechner ausführen.

> **Hinweis:** Dieser Befehl kann Dateien aus einer LAN-Dateiquelle ohne Verwendung der URL und "Agent > Agents konfigurieren > **LAN-Cache** *(siehe 78)*" herunterladen. Dateien müssen größer als 4 kB sein.

getURLUsePatchFileSource()

Lädt eine Datei von einer vorgegebenen URL in einen Zielordner und Datei für den Agent herunter. Verwendet die Patch-Management-Einstellungen > Dateiquelle.

Unterstützte Betriebssysteme: Windows

getVariable()

Definiert eine neue Agent-Variable. Beim Ausführen des Verfahrensschritts definiert das System eine neue Variable und weist ihr einen Wert zu, der auf den vom Agent auf dem verwalteten Rechner abgerufenen Daten beruht.

> **Hinweis:** Eine Liste der Arten von Variablenwerten, die vom Befehl **getVariable()** unterstützt werden, finden Sie unter **Variablen verwenden** *(siehe 120)*.

getVariableRandomNumber()

Erzeugt eine Zufallszahl, auf die dann in einem nachfolgenden Schritt als Variable `#global:rand#` zugegriffen werden kann.

Unterstützte Betriebssysteme: Windows, OS X, Linux

getVariableUniversalCreate()

Ruft eine Variable ab, die außerhalb der unmittelbaren Ausführung des Verfahrens weiter besteht. Das kann nützlich sein, wenn Sie eine Variable über den Schritt **scheduleProcedure()** auf ein anderes Agent-Verfahren verschieben wollen. Sie können bis zu drei Variablen erstellen. Sie können entweder Zeichenfolgen oder Variablen eingeben, die in in einem früheren Schritt erstellt wurden. Variablen, die über diesen Schritt erstellt wurden, können nur mithilfe des Schrittes **Variable abrufen – Universal – Lesen** in nachfolgenden Schritten gelesen werden.

Unterstützte Betriebssysteme: Windows, OS X, Linux

getVariableUniversalRead()

Liest bis zu drei zuvor über **Variable abrufen – Universal – Erstellen** erstellte Variablen. Diese Variablen können nur als `#global:universal1#`, `#global:universal2#` und `#global:universal3#` referenziert werden. Weitere Hinweise dazu finden Sie im Anfangsschritt **Variable abrufen – Universal – Erstellen**.

Unterstützte Betriebssysteme: Windows, OS X, Linux

giveCurrentUserAdminRights()

Fügt den aktuellen Benutzer zur lokalen Administratorgruppe auf dem Agent-Rechner hinzu, entweder dauerhaft oder für eine befristete Zeit. TDiese Änderung wird *nicht* wirksam, bis sich der Benutzer abmeldet. Wir empfehlen, dass Sie den Schritt **logoffCurrentUser()** nutzen.

Unterstützte Betriebssysteme: Windows

impersonateUser()

Geben Sie einen Benutzernamen, ein Kennwort und eine Domäne ein, mit denen sich der Agent anmelden kann. Dieser Befehl wird in einem Verfahren vor den Befehlen **executeFile()**, **executeFileInDirectoryPath()** oder **executeShellCommand()** verwendet, bei denen die Option **Als angemeldeten Benutzer ausführen** angegeben wird. Lassen Sie die Domäne leer, um sich bei einem Konto auf dem lokalen Rechner anzumelden. Verwenden Sie **impersonateUser()**, um ein Agent-Verfahren mithilfe von Anmeldedaten auszuführen, die *von einem Agent-Verfahren* festgelegt wurden. Mit **useCredential()** führen Sie ein Agent-Verfahren mithilfe von Anmeldedaten aus, die *von einem verwalteten Rechner* festgelegt wurden.

installAptGetPackage()

Installiert ein Paket im Hintergrund über den Befehl `apt-get` in Linux.

Unterstützte Betriebssysteme: Linux

installDebPackage()

Installiert ein Debian-Paket im Hintergrund auf jedem Linux-Betriebssystem, das `.deb`-Pakete unterstützt.

Unterstützte Betriebssysteme: Linux

installDMG()

Installiert im Hintergrund ein `.DMG`-Paket in OS X. Wenn das Paket als `Application` formatiert ist, wird es in den Ordner `/Applications` kopiert. Wenn `.DMG` ein internes `.PKG`-Installationspaket enthält, wird Kaseya versuchen, es zu installieren.

Unterstützte Betriebssysteme: OS X

installMSI()

Installiert eine MSI-Datei für Windows. Options can be selected to either run a quiet installation or to avoid automatically restarting the computer after installation if it is requested.

Unterstützte Betriebssysteme: Windows

installPKG()

Installiert im Hintergrund ein `.PKG`-Paket in OS X.

Unterstützte Betriebssysteme: OS X

installRPM()

Installiert im Hintergrund ein RPM-Paket auf jedem Linux Betriebssystem, das die Installation von RPMs unterstützt.

Unterstützte Betriebssysteme: Linux

logoffCurrentUser()

Aktueller Benutzer wird automatisch abgemeldet. Eine optionale Warnung mit dem Hinweis, dass der Abmeldungsprozess beginnt, kann eingegeben und dem Endbenutzer angezeigt werden.

Unterstützte Betriebssysteme: Windows, OS X, Linux

pauseProcedure()

Halten Sie das Verfahren für N Sekunden an. Verwenden Sie diesen Befehl, damit Windows genug Zeit zum Ausführen einer asynchronen Aufgabe hat (z. B. das Starten oder Anhalten eines Dienstes).

reboot()

Der verwaltete Rechner wird bedingungslos neu gestartet. Damit der Benutzer zuerst gewarnt wird, verwenden Sie vor diesem Befehl den Befehl **isYesFromUser()**. Der Befehl **isYesFromUser()** fordert den Benutzer vor dem Neustart seines Rechners zu einer Eingabe auf.

rebootWithWarning()

Startet einen Rechner neu und zeigt dabei dem zuvor angemeldeten Benutzer eine Warnmeldung an, bevor der Neustart beginnt.

Unterstützte Betriebssysteme: Windows, OS X, Linux

removeWindowsFileShare()

Entfernt eine Dateifreigabe von einem Windows Agent.

Unterstützte Betriebssysteme: Windows

renameLockedFile()

Benennt eine Datei um, die gegenwärtig verwendet wird. Die Datei wird beim nächsten Neustart des Systems umbenannt. Der angegebene Dateiname ist ein vollständiger Dateipfadname. Hiermit kann eine gegenwärtig verwendete Datei gelöscht werden, wenn "neuer Dateiname" leer gelassen wird. Die Datei wird beim Neustart des Systems gelöscht.

renameLockedFileInDirectoryPath()

Benennt eine Datei um, die gegenwärtig verwendet wird und sich im Pfad befindet, der von einem Befehl **getDirectoryPathFromRegistry()** zurückgegeben wurde. Die Datei wird beim nächsten Neustart des Systems umbenannt. Hiermit kann eine gegenwärtig verwendete Datei gelöscht werden, wenn "neuer Dateiname" leer gelassen wird. Die Datei wird beim Neustart des Systems gelöscht.

scheduleProcedure()

Plant ein Verfahren, das auf einem angegebenen Rechner ausgeführt werden soll. Optional können die Wartezeit zwischen Ausführung dieses Schritts und Ausführung des Verfahrens sowie die Rechner-ID zur Ausführung des Verfahrens angegeben werden. Wenn kein Rechner angegeben wird, wird das Verfahren auf demselben Rechner ausgeführt, auf dem das Agent-Verfahren läuft. Geben Sie den vollständigen Namen des Rechners ein, beispielsweise `machine.unnamed.org`. *Mithilfe dieses Befehls kann ein Agent-Verfahren, das auf einem Rechner ausgeführt wird, planen, ein Agent-Verfahren auf einem zweiten Rechner auszuführen.* Mit diesem Befehl können Sie ein **System** *(siehe 631)*verfahren ausführen. Sie können Verfahren auf 10 Ebenen verschachteln.

sendAlert()

Dieser Schrittbefehl akzeptiert keine Parameter. Stattdessen gibt mindestens ein **getVariable()** *(siehe 111)*-Schritt, *der vor dem Schritt* **sendAlert(),** *ausgeführt wurde,* die *Meldungsaktionsvariablen* an, von denen die in **sendAlert()** ausgelösten Aktionen definiert werden. Alle Meldungsaktionsvariablen sind optional. Wenn keine Meldungsaktionsvariablen definiert wurden, wird ein Alarm mit einer Systemstandardnachricht erstellt. Die Standardalarmaktion kann durch eine Meldungsaktionsvariable deaktiviert werden. Falls Meldungsaktionsvariablen verwendet werden, müssen sie den jeweiligen Aktionen entsprechende spezifische Namen verwenden:

- `alertSubject` – Betreff der Meldungsnachricht. Wenn Sie im Agent-Verfahren keine Nachricht definieren, wird eine Systemstandardnachricht ausgegeben. Siehe *Systemparameter* unten.

- `alertBody` – Text der Meldungsnachricht. Wenn Sie im Agent-Verfahren keine Nachricht definieren, wird eine Systemstandardnachricht ausgegeben. Siehe *Systemparameter* unten.
- `alertDisableAlarm` – Geben Sie bei aktiviertem Standardalarm einen beliebigen Wert ein, um ihn zu deaktivieren.
- `alertGenerateTicket` – Geben Sie einen beliebigen Wert zur Ticketerstellung ein.
- `alertScriptName` – Gültiger Name des Agent-Verfahrens, das auf dem aktuellen Rechner ausgeführt werden soll.
- `alertEmailAddressList` – Durch Kommas getrennte E-Mail-Adressen. Erforderlich für den Versand der E-Mail.
- `alertAdminNameList` – Durch Kommas getrennte Liste von VSA-Benutzernamen. Erforderlich für den Versand von Nachrichten an "Infocenter > **Posteingang** *(siehe 162)*".
- `alertNotificationBarList` – Durch Kommas getrennte Liste von VSA-Benutzernamen. Erforderlich für den Versand von Nachrichten an den **Benachrichtigungsbalken** *(siehe 11)*.
- `alertNotificationBarMasterAdmins` – Geben Sie einen beliebigen Wert ein, um Benachrichtigungen an den **Benachrichtigungsbalken** aller **Hauptbenutzer** *(siehe 410)* zu senden.

Systemparameter

Der Standardtext in `alertSubject` und `alertBody` des Befehls **sendAlert()** kann überschrieben werden. Dabei können Sie die folgenden *Systemparameter* in die Variablen `alertSubject` und `alertBody` einbetten, die Sie mithilfe der **getVariable()**-Befehle erstellen. Zur Einbettung der Parameter in den Text sind *doppelte* spitze Klammern erforderlich. Diese eingebetteten Systemparameter werden nicht mit einem **getVariable()**-Befehl erstellt. Sie sind stets verfügbar.

- <<id>> – Anzeigename des Rechners, auf dem das Agent-Verfahren ausgeführt wird
- <<gr>> – Gruppenname des Rechners, auf dem das Agent-Verfahren ausgeführt wird
- <<at>> – Datum/Uhrzeit der Meldung (Serverzeit)
- <<ata>> – Datum/Uhrzeit der Meldung (Agent-Zeit)
- <<apn>> – Name des Agent-Verfahrens, das ausgeführt wird

Benutzerdefinierte Parameter

Sie können *benutzerdefinierte Parameter* in die **getVariable()**-Befehle für `alertSubject` und `alertBody` einbetten. Erstellen Sie zunächst mit dem Befehl **getVariable()** eine weitere Variable. Der in dieser ersten Variablen gespeicherte Wert kann dynamisch sein und erst bei der Ausführung des Agent-Verfahrens festgelegt werden. Dann fügen Sie den Namen dieser ersten Variablen umgeben von `#` und `#` in den Textwert ein, der von den **getVariable()**-Befehlen für `alertSubject` und `alertBody` angegeben wurde. Beispiele:

- `#filename#`
- `#logentry#`
- `#registrykey#`
- `#registryvalue#`

Festlegen von getVariable()-Befehlen vor sendAlert() in einem Agent-Verfahren

Angenommen:

1. Ein Agent-Verfahren erstellt eine Variable namens `runTimeVar` mithilfe des Befehls **getVariable()**. Die eingegebenen Werte lauten:
   - `Constant Value`
   - `Procedure terminated. Could not access 'File Server 123'.`
   - `runTimeVar`
   - `All Operating Systems`
   - `Continue on Fail`

2. Anschließend wird im selben Verfahren ein zweiter **getVariable()**-Befehl generiert. Dieser zweite **getVariable()**-Befehl legt den *Textkörper* (Body) einer **sendAlert()**-Nachricht fest. Im Textkörper sind sowohl System- als auch benutzerdefinierte Parameter eingebettet. Die für den zweiten **getVariable()**-Befehl eingegebenen Werte sind:
   - `Constant Value`
   - This alert was generated by <<apn>> on machine <<id>> at <<ata>>: #runTimeVar#.
   - `alertBody`
   - `All Operating Systems`
   - `Continue on Fail`
3. Schließlich wird der Befehl **sendAlert()** ausgeführt und die Meldungsnachricht erstellt.

> **Hinweis:** Die Reihenfolge der Parametervariablen und Meldungsaktionsvariablen spielt keine Rolle. *Es müssen allerdings alle ausgeführt worden sein, bevor sie im Befehl sendAlert() genutzt werden.*

sendEmail()

Sendet eine E-Mail an einen oder mehrere Empfänger. Geben Sie den Betreff und Textkörper der E-Mail-Nachricht an.

sendMessage()

Sendet die eingegebene Nachricht an einen verwalteten Rechner. Zusätzliches Kontrollkästchen: Wenn angekreuzt, wird die Nachricht sofort gesendet. Falls ein zusätzliches Kontrollkästchen aktiviert wird, wird die Nachricht gesendet, nachdem der Benutzer auf das blinkende Agent-Symbol in der Systemablage geklickt hat.

sendURL()

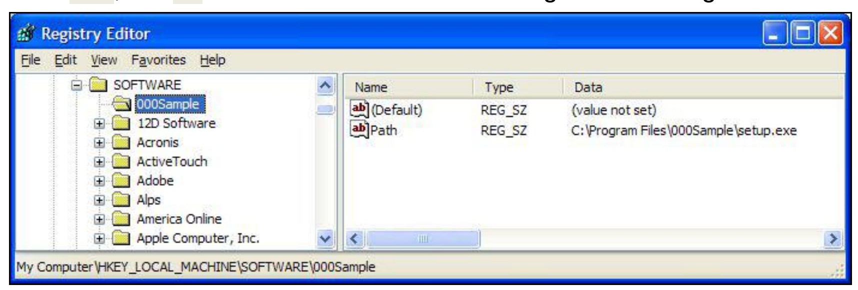
Zeigt die eingegebene URL in einem Webbrowserfenster auf dem verwalteten Rechner an. Zusätzliches Kontrollkästchen: Wenn angekreuzt, wird die URL sofort angezeigt. Falls ein zusätzliches Kontrollkästchen aktiviert wird, wird die URL angezeigt, nachdem der Benutzer auf das blinkende Agent-Symbol in der Systemablage geklickt hat.

setRegistryValue()/set64BitRegistryValue() *(siehe 119)*

Schreibt Daten in den angegebenen Registrierungswert. Diese Funktion braucht drei Parameter:

- **Geben Sie den vollständigen Pfad zu einem Registry-Schlüssel ein, der einen Wert enthält.**
  - Geben Sie den `(Default)`-Wert für einen Registrierungsschlüssel ein, indem Sie einen umgekehrten Schrägstrich `\` anhängen. Geben Sie ansonsten einen Namen für einen vorhandenen Wert ein oder erstellen Sie einen neuen Wert. Siehe Spalte `Name` in der unten stehenden Abbildung.
    Beispiel der Einstellung des `(Default)`-Werts:
    `HKEY_LOCAL_MACHINE\SOFTWARE\000Sample\`
  - Der *letzte einzelne Schrägstrich* in einer Zeichenfolge dient zur Abgrenzung des Registrierungsschlüssels vom Registrierungswert. Wenn Ihre Zeichenfolge Schrägstriche enthalten soll, müssen diese als *doppelte Schrägstriche* angegeben werden. Die Zeichenfolge `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Value\\Name` wird beispielsweise als Schlüssel namens `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey` mit dem Wert `Value\Name` interpretiert.
- **Geben Sie die Daten ein, die in den Registrierungswert geschrieben werden sollen.**
- **Datentyp auswählen**
  - `REG_SZ` – Zeichenfolgewert

- REG_BINARY – Binärdaten im hexadezimalen Format
- DWORD – Auf 32 Bit beschränkte Binärdaten. Kann im hexadezimalen oder dezimalen Format eingegeben werden.
- REG_EXPAND_SZ – Eine "erweiterbare" Zeichenfolge, die eine Variable enthält. Beispiel: %SystemRoot%.
- REG_MULTI_SZ – Eine Aufstellung mehrerer Zeichenfolgen. Wird zur Eingabe von mehreren Werten verwendet, die jeweils durch die Zeichenfolge \0 getrennt werden. Verwenden Sie \\0, um \0 in den Wert einer Zeichenfolgenaufstellung einzuschließen.



sqlRead()

Gibt einen Wert aus einer Datenbank zurück und speichert ihn durch Ausführung eines ausgewählten SQL-"Read"-Befehls in einer umbenannten Variablen. Globale "Read"-Anweisungen werden an folgendem Ort definiert: <KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\0\SQLRead\<filename.xml> Dateinamen können beliebige Namen mit der Erweiterung .xml sein, vorausgesetzt, sie sind intern korrekt formatiert. Wenn durch eine oder mehrere XML-Datei(en) mehrere Anweisungen definiert werden, werden diese in der Benutzeroberfläche in einer gemeinsamen Kombinationsfeldliste angezeigt. Jede SQL-Anweisung in der XML-Datei weist eine eigene Bezeichnung auf; nur die Bezeichnungen werden im Kombinationsfeld angezeigt. Wenn keine SQL-Anweisungen definiert sind, wird im Kombinationsfeld der Eintrag *No Approved SQL* angezeigt.

Partitionsspezifische Anweisungen

Partitionsspezifische Ordner können partitionsspezifische SQL-Anweisungen enthalten. Zum Beispiel: <KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\123456789\SQLRead\<filename.xml>. Benutzer können alle SQL-"Read"-Anweisungen im Ordner 0 und im eigenen Partitionspfad auswählen und ausführen.

Beispielformat

```
<?xml version="1.0" encoding="utf-8" ?>
<queryList>
   <queryDef label="Agent Machine Name" sql="SELECT machName FROM dbo.machNameTab WHERE agentGuid = #vMachine.agentGuid#" />
</queryList>
```

sqlWrite()

Aktualisiert die Datenbank (etwa durch Aktualisierung eines Werts in einer Spalte oder Hinzufügen einer Zeile) über einen ausgewählten SQL-"Write"-Befehl. Globale "Write"-Anweisungen werden an folgendem Ort definiert: <KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\0\SQLWrite\<filename.xml> Dateinamen können beliebige Namen mit der Erweiterung .xml sein, vorausgesetzt, sie sind intern korrekt formatiert. Wenn durch eine oder mehrere XML-Datei(en) mehrere Anweisungen definiert werden, werden diese in der Benutzeroberfläche in einer gemeinsamen Kombinationsfeldliste angezeigt. Jede SQL-Anweisung in der XML-Datei weist eine eigene Bezeichnung auf; nur die Bezeichnungen werden im Kombinationsfeld angezeigt. Wenn keine SQL-Anweisungen definiert sind, wird im Kombinationsfeld der Eintrag *No Approved SQL* angezeigt.

Partitionsspezifische Anweisungen

Partitionsspezifische Ordner können partitionsspezifische SQL-Anweisungen enthalten. Zum Beispiel: <KaseyaInstallationDirectory>\xml\Procedures\AgentProcSQL\123456789\SQLWrite\<filename.xml>. Benutzer können alle SQL-"Write"-Anweisungen im Ordner 0 und im eigenen Partitionspfad auswählen und ausführen.

Beispielformat

```
<?xml version="1.0" encoding="utf-8" ?>
<queryList>
   <queryDef label="Update Table" sql="UPDATE table1 SET column2 = value2 WHERE column1 = value1" />
</queryList>
```

startWindowsService()

Führt einen Startbefehl für einen Windows Service aus, sofern er existiert.

Unterstützte Betriebssysteme: Windows

stopWindowsService()

Führt einen Startbefehl für einen Windows Service aus, sofern er existiert.

Unterstützte Betriebssysteme: Windows

transferFile()

Überträgt eine Datei von dem Agent-Rechner, der gerade diesen Schritt ausführt, auf einen anderen Agent-Rechner. Geben Sie die vollständig qualifizierte Rechner-ID des *Zielrechners* ein, z. B. mymachine.root.kaseya. Geben Sie anschließend den vollständigen Pfad- und Dateinamen der Quelldatei ein, die Sie *über den aktuell ausgewählten Agent* senden möchten. Schließlich geben Sie den vollständigen Pfad- und Dateinamen der Zieldatei auf dem Zielrechner ein.

Unterstützte Betriebssysteme: Windows

uninstallbyProductGUID()

Deinstalliert im Hintergrund ein Produkt auf Basis seiner MSI-GUID.

Unterstützte Betriebssysteme: Windows

unzipFile()

Extrahiert den Inhalt einer bestimmten Zip-Datei in einen Zielordner mit einer Option zum automatischen Überschreiben bestehender Zieldateien oder Zielordner.

Unterstützte Betriebssysteme: Windows, OS X, Linux

updateSystemInfo()

Aktualisiert das Feld **Systeminformationen** mit dem angegebenen Wert für die Rechner-ID, auf der dieses Verfahren ausgeführt wird. Die Felder in **Systeminformationen**, die Sie aktualisieren können, umfassen alle Spalten in **vSystemInfo** *(siehe 524)* außer agentGuid, emailAddr, Machine_GroupID, machName und groupName. Die Spalteninformationen in **vSystemInfo** werden von "Audit > **Systeminformationen** *(siehe 154)*", "Agent > **Systemstatus** *(siehe 32)*", der **Filtergesamttabelle** *(siehe 30)* in **Ansichtsdefinitionen** und dem Bericht **Gesamttabelle** *(siehe 206)* verwendet. Sie können ein Feld in **Systeminformationen** mit jedem Zeichenfolgenwert aktualisieren, einschließlich des Werts einer bereits definierten Agent-Verfahrensvariable.

useCredential()

Verwendet die Anmeldedaten, die in **Anmeldedaten einstellen** *(siehe 77)* für die Rechner-ID festgelegt wurden. Dieser Befehl wird in einem Verfahren vor den Befehlen **executeFile()**, **executeFileInDirectoryPath()** oder **executeShellCommand()** verwendet, bei denen die Option **Als angemeldeten**

Benutzer ausführen angegeben wird. Dies wird ebenfalls beim Zugriff auf eine Netzwerkressource verwendet, die Anmeldedaten von einem Rechner erfordert, wenn kein Benutzer angemeldet ist. Verwenden Sie **impersonateUser()**, um ein Agent-Verfahren mithilfe von Anmeldedaten auszuführen, die *von einem Agent-Verfahren* festgelegt wurden. Mit **useCredential()** führen Sie ein Agent-Verfahren mithilfe von Anmeldedaten aus, die *von einem verwalteten Rechner* festgelegt wurden.

> **Hinweis:** Wenn ein Verfahrensbefehl **Anmeldedaten einstellen** auf einen leeren Benutzernamen trifft, wird ein Verfahrensausführungsfehler im Protokoll verzeichnet.
>
> **Hinweis:** Patch-Management > Patch-Meldung kann Sie warnen (oder ein Agent-Verfahren ausführen), wenn die Anmeldedaten einer Rechner-ID fehlen oder ungültig sind.

windowsServiceRecoverySettings()

Richtet die Einstellungen für Service-Wiederherstellungen für jeden beliebigen Windows Service ein. Geben Sie den Namen des Diensts ein, den Sie ändern möchten, und legen Sie dann die Fehleroptionen für den ersten und den zweiten Neustart sowie jene für alle darauffolgenden Neustarts fest.

Unterstützte Betriebssysteme: Windows

writeDirectory()

Schreibt ein ausgewähltes Verzeichnis, einschließlich Unterverzeichnisse und Dateien, von **Auf dem Server gespeicherte Dateien verwalten** *(siehe 124)* in den vollständigen, auf dem verwalteten Rechner angegebenen Pfadverzeichnisnamen.

writeFile()

Schreibt eine bei **Auf dem Server gespeicherte Dateien verwalten** *(siehe 124)* ausgewählte Datei in den vollständigen, auf dem verwalteten Rechner angegebenen Pfadverzeichnisnamen. Geben Sie einen neuen Dateinamen ein, wenn die Datei umbenannt werden soll.

Bei jeder Ausführung des Befehls **writeFile()** durch ein Verfahren prüft der Agent, ob die Datei bereits vorhanden ist, indem er die Integrität der Datei durch Hash-Codierung überprüft. Wenn die Datei nicht vorhanden ist, wird sie geschrieben. Ist sie bereits vorhanden, geht das Verfahren zum nächsten Schritt über. Mit **writeFile()** können Sie ein Verfahren wiederholt ausführen, das eine große Datei an einen verwalteten Rechner sendet, und sicher sein, dass der VSA diese Datei nur einmal herunterlädt.

> **Hinweis:** Umgebungsvariablen sind zulässig, wenn sie auf dem Rechner eines Benutzers eingestellt sind. Zum Beispiel entspricht die Verwendung des Pfads `%windir%\notepad.exe` dem Pfad `C:\windows\notepad.exe`.
>
> **Hinweis:** Dieser Befehl kann Dateien aus einer LAN-Dateiquelle ohne Verwendung des VSA und "Agent > Agents konfigurieren > **LAN-Cache** *(siehe 78)*" herunterladen. Dateien müssen größer als 4 kB sein.

writeFileFromAgent()

Überträgt eine Datei von einem anderen Agent-Rechner auf den Agent-Rechner, der gerade diesen Schritt ausführt. Überträgt eine Datei von einem Agent zum anderen. Ähnlich wie der vorherige Schritt, **transferFile()**, wobei Sie hier jedoch die vollständig qualifizierte Rechner-ID des *Quellrechners* angeben, auf dem die Datei gespeichert ist, die an den *aktuell ausgewählten Agent gesendet werden soll.* Geben Sie zunächst den vollständigen Pfad- und Dateinamen der Datei ein, die Sie über vom Quellrechner versenden möchten. Geben Sie anschließend den vollständigen Pfad- und Dateinamen an, der auf dem Zielrechner erstellt werden soll.

Unterstützte Betriebssysteme: Windows

writeFileInDirectoryPath()

Schreibt den angegebenen Dateinamen in den Pfad, der vom Befehl **getDirectoryPathFromRegistry()** zurückgegeben wurde.

writeProcedureLogEntry()

Schreibt die gelieferte Zeichenfolge in das Agent-Verfahrensprotokoll für die Rechner-ID, auf der dieses Agent-Verfahren ausgeführt wird.

writeTextToFile()

Schreibt Text in eine Datei auf dem Agent-Rechner, entweder durch Anhängen von Text an eine bestehende Datei oder durch Erstellung einer neuen Datei, wenn keine vorhanden ist. Sie geben den gewünschten Text ein und legen anschließend den vollständigen Pfad- und Dateinamen der Datei auf dem Agent-Rechner fest, in die der Text geschrieben werden soll. Optional können Sie die gesamte Datei mit dem Text überschreiben, falls die Datei bereits vorhanden ist.

Unterstützte Betriebssysteme: Windows, OS X, Linux

zipDirectory()

Komprimiert ein Verzeichnis und jegliche Unterverzeichnisse oder Dateien, die es enthält, in eine Zip-Datei auf dem Agent-Rechner. Geben Sie den vollständigen Pfad ein, der komprimiert werden soll. Der Pfad darf Platzhalter enthalten. Geben Sie anschließend den vollständigen Pfad- und Dateinamen der Zip-Datei ein, die erstellt oder aktualisiert werden soll. Wenn die Zieldatei bereits vorhanden ist, können Sie optional ein Kontrollkästchen aktivieren, um sie zu überschreiben.

Unterstützte Betriebssysteme: Windows, OS X, Linux

zipFiles()

Komprimiert eine einzige Datei oder Dateien in eine Zip-Datei auf dem Agent-Rechner. Geben Sie den vollständigen Pfad der zu komprimierenden Datei bzw. Dateien ein. Geben Sie anschließend den vollständigen Pfad- und Dateinamen der Zip-Datei ein, die erstellt oder aktualisiert werden soll. Wenn die Zieldatei bereits vorhanden ist, können Sie optional ein Kontrollkästchen aktivieren, um sie zu überschreiben.

Unterstützte Betriebssysteme: Windows, OS X, Linux

64-Bit-Befehle

Auf 64-Bit-Registrierungswerte zugreifen

In Agent-Verfahren stehen fünf 64-Bit-Registrierungsbefehle und ein 64-Bit-Parameter zur Verfügung. 64-Bit-Windows isoliert die Registrierungsnutzung durch 32-Bit-Anwendungen, indem es eine separate logische Ansicht der Registrierung bereitstellt. Die Umleitung zur separaten logischen Ansicht wird automatisch aktiviert und ist für die folgenden Registrierungsschlüssel transparent:

- `HKEY_LOCAL_MACHINE\SOFTWARE`
- `HKEY_USERS\*\SOFTWARE\Classes`
- `HKEY_USERS\*_Classes`

Da es sich beim Kaseya Agent um eine 32-Bit-Anwendung handelt, müssen Sie mithilfe der folgenden Befehle und Parameter auf die Registrierungsdaten zugreifen, die von den 64-Bit-Anwendungen in den oben genannten Schlüsseln gespeichert werden.

IF-Befehle

- get64BitRegistryValue()
- has64bitRegistryKey()

SCHRITT-Befehle

- delete64BitRegistryValue()
- delete64BitRegistryKey()
- set64BitRegistryValue()
- 64-Bit-Registrierungswertparameter im Befehl "getVariable()"

64-Bit-Pfade in Dateibefehlen angeben

Die folgenden Befehle...

- **deleteFile()**
- **writeFile()**
- **executeFile()**
- **renameLockedFile()**
- **getFile()**
- Parameter **get-variable()** `File Content`

... können unter Verwendung der folgenden Variablen 64-Bit-Verzeichnisse angeben:

Diese Umgebungsvariable verwenden	Für Zielverzeichnis
`%windir%\sysnative`	`<drive>:\Windows\System32`
`%ProgramW6432%`	`<drive>:\Program Files`
`%CommonProgramW6432%`	`<drive>:\Program Files\Common Files`

Aus Gründen der Kompatibilität hat Microsoft 64-Bit-Systemdateien im Verzeichnis `\Windows\system32` und 32-Bit-Systemdateien im Verzeichnis `\Windows\SysWOW64` abgelegt. Ebenso sind 64-Bit-Anwendungsdateien im Ordner `\Program Files` und 32-Bit-Anwendungsdateien im Ordner `\Program Files (x86)` installiert. Da der Kaseya-Agent eine 32-Bit-Anwendung ist, wird der Dateizugriff bei Angabe eines Pfads mit `\Windows\system32` oder `\Program Files` auf einem 64-Bit-Rechner automatisch zu den Ordnern `\Windows\SysWOW64` oder `\Program Files (x86)` umgeleitet. Verwenden Sie bei der Angabe von Parametern für diese Dateibefehle diese Umgebungsvariablen, um auf Dateien in den Ordnern `\Windows\system32` und `\Program Files` zuzugreifen.

In Verzeichnispfadbefehlen

Auf einem 64-Bit-Zielrechner kann der Befehl **getDirectoryPathFromRegistry()** (und jeder nachfolgende Befehl **...In Verzeichnispfad**) nicht für den Zugriff auf Dateien in den Verzeichnissen `\Program Files` und `\Windows\System32` verwendet werden. Diese Befehle können jedoch weiterhin auf 32-Bit- oder 64-Bit-Dateien in allen anderen Ordnern zugreifen.

64-Bit-Rechner identifizieren

Die ID eines 64-Bit-Rechners wird normalerweise mit einem `x64` in der Spalte **Version** der Audit-Seiten angezeigt.

Variablen verwenden

Mithilfe von Variablen können Sie Werte speichern, auf die in mehreren Verfahrensschritten verwiesen werden kann. Variablen werden automatisch an verschachtelte Verfahren übergeben.

- **Zwei Methoden zum Erstellen von Variablen:**
  - **Verfahrensvariablen** – Verwenden Sie den Befehl **getVariable()** in einem Verfahren, um einen neuen Variablennamen ohne Sonderzeichen zu erstellen. Beispiel: `VariableName`. In nachfolgenden Schritten, auch jenen in verschachtelten Verfahren, verweisen Sie auf den Variablennamen mit dem Zeichen `#`. Beispiel: `#VariableName#`.

> **Hinweis:** *Außer im Fall von GLOBAL-Variablen können Verfahrensvariablen nicht außerhalb desselben Verfahrens bzw. derselben verschachtelten Verfahren referenziert werden.* Eine Verfahrensvariable ist nur in dem Abschnitt des Verfahrens und allen untergeordeneten Verfahren sichtbar, in dem sie erstellt wurde. Sobald ein Verfahren die THEN- oder ELSE-Klausel verlässt, in dem die Variable erstellt wurde, fällt die Variable aus dem Bereich heraus und ist nicht länger gültig. Verwenden Sie wie unten beschreiben *GLOBALE Variablen*, damit die Variable nach Verlassen der THEN- oder ELSE-Klausel, in der sie erstellt wurde, weiter sichtbar ist.

- **Verwaltete Variablen** – Verwenden Sie den **Variablen-Manager** *(siehe 123)*, um Variablen zu definieren, die wiederholt in verschiedenen Verfahren verwendet werden können. Sie können mehrfache Werte für jede verwaltete Variable pflegen. Jeder Wert wird auf eine oder mehrere Gruppen-IDs angewendet. Verwalteten Variablen können keine neuen Werte innerhalb eines Verfahrens zugewiesen werden. In einem Verfahren verweisen Sie auf eine verwaltete Variable, indem Sie den Variablennamen mit den Zeichen `<` und `>` einklammern. Beispiel: <VariableName>.
- **GLOBALE Variablen** – Nicht-GLOBALE Variablen können keinen geänderten Wert einer Verfahrensvariablen, die durch ein übergeordnetes Verfahren definiert wurde, zurückgeben. Nicht-GLOBALE Variablen, die im untergeordneten Verfahren initialisiert wurden, können ebenfalls nicht zum übergeordneten Verfahren zurückgegeben werden. Variablennamen mit dem Präfix `GLOBAL:` (keine Unterscheidung zwischen Groß- und Kleinschreibung, mit anschließendem Doppelpunkt) können geänderte Werte vom untergeordneten in das übergeordnete Verfahren zurückgeben, ganz gleich, ob die Variable im übergeordneten oder untergeordneten Verfahren initialisiert wurde. Nachfolgende untergeordnete Verfahren können jede GLOBALE Variable verwenden, die in einem früheren Schritt initialisiert wurde, ganz gleich, ob diese globale Variable in einem übergeordneten Verfahren oder einem anderen untergeordneten Verfahren initialisiert wurde.

- **Variablennamen** – *Variablennamen* dürfen keine der folgenden Zeichen enthalten: `, % ' " / \ : * ? < > |` und Leerzeichen.
- **Verwendungsbereich** – Nach der Erstellung von Variablen können diese im Klammernformat *in jedes Texteingabefeld* eingeschlossen werden, das in einem IF-ELSE--SCHRITT-Dialogfeld angezeigt wird.
- **Groß-/Kleinschreibung** – Bei Variablennamen muss auf Groß-/Kleinschreibung geachtet werden.
- **Reservierte Zeichen** – Da die Zeichen `<`, `>` und `#` zur Kennzeichnung von Variablennamen verwendet werden, müssen diese Zeichen *zweimal* als normaler Text in eine Befehlszeile eingegeben werden. Beispielsweise wird der Befehl `c:\dir >> filelist.txt` bei Ausführung des Verfahrens als `c:\dir > filelist.txt` interpretiert.
- **Mögliche Arten von Variablenwerten** – Es folgen die Arten von Variablenwerten, die normalerweise bei Verwendung des Parameters **getVariable()** abgerufen werden.
  - **Registrierungswert** und **64-Bit-Registrierungswert** – Siehe **64-Bit-Befehle** *(siehe 119)* – Daten aus dem angegebenen Registrierungswert auf dem verwalteten Rechner. Der *letzte einzelne Schrägstrich* in einer Zeichenfolge dient zur Abgrenzung des Registrierungsschlüssels vom Registrierungswert. Wenn Ihre Zeichenfolge Schrägstriche enthalten soll, müssen diese als *doppelte Schrägstriche* angegeben werden. Die Zeichenfolge `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey\Value\\Name` wird beispielsweise als Schlüssel namens `HKEY_LOCAL_MACHINE\SOFTWARE\SomeKey` mit dem Wert `Value\Name` interpretiert.
  - **Dateiinhalt** – Daten aus einer angegebenen Datei auf dem verwalteten Rechner Siehe **64-Bit-Befehle** *(siehe 119)*.
  - **Konstantenwert** – Die angegebene Konstante, so wie sie im Verfahrenseditor eingegeben wurde
  - **Installationsverzeichnispfad für den Agent** – Das Verzeichnis, in dem der Agent auf dem verwalteten Rechner installiert ist

- **Agent-Installationslaufwerk** – Das Laufwerk, auf dem der Agent auf dem verwalteten Rechner installiert ist, z. B. `c:\`
- **Pfad für Arbeitsverzeichnis des Agents** – Das Arbeitsverzeichnis auf dem verwalteten Rechner, das über Agent > **Working Directory** *(siehe 72)* festgelegt wurde.

> **Warnung: Löschen Sie keine Dateien und Ordner im Arbeitsverzeichnis.** Der Agent verwendet die im Arbeitsverzeichnis gespeicherten Daten, um verschiedene Aufgaben auszuführen.

- **Benutzer temporäres Verzeichnis** – Das temporäre Verzeichnis des Benutzers, der gegenwärtig am verwalteten Rechner angemeldet ist. Dieser Pfad ist die Erweiterung der Umgebungsvariablen `%TEMP%` für den gegenwärtig angemeldeten Benutzer. Falls kein Benutzer angemeldet ist, stellt dies das standardmäßige temporäre Windows-Verzeichnis dar.
- **Rechner-Gruppen-ID** – Dies ist die Rechner-ID des Agents, der das Verfahren ausführt.
- **Versionsnummer der Datei** – Die Softwareversionsnummer der angegebenen Datei auf dem verwalteten Rechner. Zum Beispiel enthält eine `exe`- oder `dll`-Datei häufig die Nummer ihrer Version.
- **Dateigröße** – Dies ist die Größe (in Byte) der angegebenen Datei auf dem verwalteten Rechner.
- **Letztes Änderungsdatum der Datei** – Dies ist das Datum und die Uhrzeit der letzten Änderung in koordinierter Weltzeit (UTC) der angegebenen Datei auf dem verwalteten Rechner im Format `yyyy/mm/dd hh:mm:ss`.
- **Automatische SQL-Ansichtsdatenvariablen** – SQL-Ansichtsparameter sind als automatisch deklarierte Verfahrensvariablen verfügbar. Automatische Variablen ermöglichen Ihnen den Befehl **Variable abrufen** zu überspringen, bevor Sie die Variable in einem SCHRITT einsetzen. Verwenden Sie das Format `#SqlViewName.ColumnName#` in einem Verfahren, um den Wert einer **dbo.SqlView.Column** *für den Agent zurückzugeben, der das Agent-Verfahren ausführt*. Eine Liste der verfügbaren SQL-Ansichten und Spalten finden Sie unter System > **Datenbankansichten** *(siehe 479)*.

  > **Hinweis: SQL-Ansichtsdaten** – Dieses ältere Verfahren zur Rückgabe eines Datenbankansichtswerts ist nur erforderlich, wenn Sie versuchen, einen Wert von *anderen Rechnern, auf denen das Agent-Verfahren nicht ausgeführt wird*, zurückzugeben.
  >
  > Verwenden Sie den Befehl **Variable abrufen** mit der Option **SQL-Ansichtsdaten**, um eine neue Verfahrensvariable zu erstellen und auf den Wert eines **dbo.SqlAnsicht.Spalte**-Wertes einzustellen. Verwenden Sie das Format `SqlViewName/ColumnName/mach.groupID` oder `SqlViewName/ColumnName`. Wenn die optionale Rechner-ID weggelassen wird, wird der Wert für den Agent abgerufen, der das Verfahren ausführt. Falls `ColumnName` eine Leerstelle enthält, schließen Sie sie in eckige Klammern ein. Beispiel: `vSystemInfo/[Product Name]`. Unter "System > **Datenbanksichten** *(siehe 479)* finden Sie eine Liste der verfügbaren SQL-Ansichten und Spalten.

- **Automatische Administrator-Variablen** – Drei Administrator-Variablen werden automatisch festgestellt. Dieese automatischen Administrator-Variablen ermöglichen, dass Agent-Verfahren Zugriff auf Werte haben, die nicht in einer SQL-Ansicht angezeigt werden.
  - ✓ `#adminDefaults.adminEmail#` – E-Mail-Adresse des VSA-Benutzers, der das Agent-Verfahren geplant hat
  - ✓ `#adminDefaults.adminName#` – Name des VSA-Benutzers, der das Agent-Verfahren geplant hat
  - ✓ `#scriptIdTab.scriptName#` – Name des Agent-Verfahrens
- **WMI -Eigenschaft** – WMI-Adressraum, -Klasse und -Eigenschaft. Das Format der angegeben WMI-Eigenschaft lautet `NameSpace:Class.Property`. Beispiel:

`root\cimv2:Win32_OperatingSystem.FreePhysicalMemory`. Geben Sie eine Instanz in der folgenden Syntax an: `NameSpace:Class[N].Property`, wobei `[N]` die Instanznummer ist. Beispiel: `root\cimv2:Win32_OnboardDevice[3].Description`. Die erste Instanz kann mit oder ohne Instanznummer `[1]` angegeben werden.

- **Ausdruckswert** – Geben Sie einen Ausdruck an, der aus Verfahrensvariablen und den sechs mathematischen Operatoren `+`, `-`, `*`, `/`, `(` und `)` besteht, die bewertet und einer neuen Verfahrensvariable zugewiesen werden. Beispiel: `((#variable1# + #variable2#) + 17.4) / (#variable3# * 4)`. Die Verfahrensvariablen müssen numerische Werte enthalten.
- **Aufforderung, wenn Verfahren geplant ist** – Sie werden in einer Meldung zur Eingabe eines Werts aufgefordert, wenn ein Agent-Verfahren ausgeführt wird. Der Wert wird im angegebenen Variablennamen gespeichert. Geben Sie den Aufforderungstext und Variablennamen ein. Beispielsweise könnte ein VSA-Benutzer bei jeder Ausführung dieses Verfahrens ein anderes Rechnerverzeichnis eingeben.

- **Meldungsvariablen** – Ein Agent-Verfahren kann so zugewiesen werden, dass es bei Auslösung einer Meldung ausgelöst wird. In den meisten Fällen übergibt die Meldung vordefinierte Werte an das Agent-Verfahren. Diese Meldungsvariablen werden nach Thema dokumentiert. Ein Beispiel dafür finden Sie unter **Meldungen – Neuer Agent installiert** *(siehe 304)*.
- **Windows-Umgebungsvariablen** – Windows-Umgebungsvariablen können ausschließlich in den Befehlen **executeFile()**, **Datei im Verzeichnispfad ausführen** und **executeShellCommand()** referenziert werden. Umschließen Sie den gesamten Befehl mit Ausführungszeichen, denn die Umgebungsvariable kann Leerschritte enthalten, die die Ausführung beeinträchtigen können. Für andere Agent-Verfahren-Befehle nutzen Sie **getVariable()**, um den Registrierungsschlüssel mit der Umgebungsvariablen aus `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment` abzurufen.

Variable Manager

Verwenden Sie den **Variable Manager**, um Variablen zu definieren, die wiederholt in verschiedenen Agent-Verfahren verwendet werden können. Sie können mehrfache Werte für jede verwaltete Variable pflegen. Jeder Wert wird auf eine oder mehrere Gruppen-IDs angewendet. Verwalteten Variablen können keine neuen Werte innerhalb eines Verfahrens zugewiesen werden. In einem Verfahren verweisen Sie auf eine verwaltete Variable, indem Sie den Variablennamen mit den Zeichen `<` und `>` einklammern. Beispiel: `<VariableName>`. Siehe **Variablen verwenden** *(siehe 120)*.

Mithilfe von verwalteten Variablen können verwaltete Rechner Agent-Verfahren ausführen, die basierend auf der Gruppen- oder Untergruppen-ID auf *lokal verfügbare Ressourcen* zugreifen.

> **Hinweis:** Unter "System > **Benennungsrichtlinie** *(siehe 406)*" kann dies automatisch nach IP-Adresse angewendet werden, selbst für höchst mobile Mitarbeiter, die regelmäßig zwischen verschiedenen Unternehmensstandorten reisen.

Variable auswählen

Wählen Sie einen Variablennamen aus der Dropdown-Liste aus oder wählen Sie `<New Variable>`, um eine neue Variable zu erstellen. *Variablennamen* **beachten die Groß- Kleinschreibung** und dürfen keine der folgenden Zeichen enthalten: `, % ' " / \ : * ? < > |` und Leerzeichen.

Variable umbenennen/erstellen

Geben Sie einen neuen Namen für die neu erstellte Variable oder für eine vorhandene Variable ein, die Sie umbenennen. Klicken Sie auf das Löschsymbol, um die ganze Variable aus allen Gruppen zu löschen.

Öffentlich

Durch Auswahl der Optionsschaltfläche **Öffentlich** kann die Variable von allen Benutzern verwendet werden. Gemeinsam genutzte Variablen können jedoch nur von Benutzern mit Master-Rolle erstellt und bearbeitet werden.

Persönlich

Bei Auswahl der Optionsschaltfläche **Privat** kann die Variable nur von dem Benutzer verwendet werden, der sie erstellte.

Anwenden

Geben Sie den Anfangswert für eine Variable ein. Wählen Sie dann eine oder mehrere **Gruppen-IDs** aus und klicken Sie auf **Anwenden**. Leere Werte sind nicht zulässig.

Entfernen

Wählen Sie eine oder mehrere Gruppen-IDs aus und klicken Sie dann auf **Löschen**, um den Wert für diese Variable aus den Gruppen-IDs zu entfernen, denen sie zugewiesen ist.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Gruppen-ID

Zeigt alle Gruppen-IDs an, die der angemeldete Benutzer verwalten darf.

Wert

Listet den Wert der Variable auf, die der Gruppen-ID zugewiesen ist.

Auf dem Server gespeicherte Dateien verwalten

Agent-Verfahren > Verfahren verwalten > Planen/Erstellen > Dateien verwalten

Im Popup-Fenster **Auf dem Server gespeicherte Dateien verwalten** können Sie eine Datei hochladen und auf dem Kaseya Server speichern. Außerdem können Sie bereits auf dem Kaseya Server gespeicherte Dateien auflisten, anzeigen und löschen. Agent-Verfahren können diese Dateien unter Verwendung der Befehle **writeFile()** oder **writeFileInDirectoryPath()** an verwaltete Rechner verteilen.

> **Hinweis:** Dieser Dateispeicher ist nicht rechnerspezifisch. **getFile()** *(siehe 134)* lädt und speichert rechnerspezifische Dateien auf dem Server.

So laden Sie eine Datei hoch:

- Klicken Sie auf **Persönliche Dateien** oder **Gemeinsam genutzte Dateien**, um den Ordner auszuwählen, in dem hochgeladene Dateien gespeichert werden. Die im Ordner **Persönliche Dateien** gespeicherten Dateien können nicht von anderen Benutzern gesehen werden.
- Klicken Sie auf **Blättern...**, um nach hochzuladenden Dateien zu suchen. Klicken Sie anschließend auf **Hochladen**, um die Datei auf den Kaseya Server hochzuladen.

  > **Hinweis:** Sie können die maximal zulässige Dateigröße für den Upload ändern.

So löschen Sie eine auf dem Kaseya Server gespeicherte Datei:

- Klicken Sie auf **Persönliche Dateien** oder **Gemeinsam genutzte Dateien**, um den Ordner auszuwählen, in dem hochgeladene Dateien gespeichert werden.
- Klicken Sie auf das Löschsymbol ✗ neben einem Dateinamen, um diese Datei vom Kaseya Server zu löschen.

> **Hinweis:** Als alternative Methode zum Hochladen von Dateien können Sie sie direkt in das Verzeichnis für verwaltete Dateien auf dem IIS-Server kopieren. Dieses Verzeichnis befindet sich normalerweise unter `C:\Kaseya\WebPages\ManagedFiles`. Dieses Verzeichnis umfasst mehrere Unterverzeichnisse. Legen Sie persönliche Dateien im Verzeichnis mit dem Namen des jeweiligen Benutzers ab. Speichern Sie gemeinsam genutzte Dateien im Verzeichnis `VSASharedFiles`. Bei der nächsten Benutzeranmeldung werden alle Dateien in diesem Verzeichnis automatisch mit dem in der Benutzeroberfläche **Auf dem Server gespeicherte Dateien verwalten** verfügbaren Material aktualisiert.

Ordnerrechte

Private Ordner

Von Ihnen erstellte Objekte, z. B. Berichte, Verfahren oder Monitorsets, werden anfänglich in einem Ordner mit Ihrem Benutzernamen unterhalb eines **Privat**-Cabinet gespeichert. Dies bedeutet, dass nur Sie, der Ersteller der Objekte in diesem Ordner, diese Objekte anzeigen, bearbeiten, ausführen, löschen oder umbennen können.

Um ein privates Objekt an andere Benutzer freizugeben, müssen Sie es zuerst in einen Ordner unterhalb des Cabinet **Gemeinsam nutzen** ziehen und dort ablegen.

> **Hinweis:** Ein Benutzer mit Master-Rolle kann das Kontrollkästchen **Freigegebene und private Ordnerinhalte aller Benutzer anzeigen** unter "System > **Voreinstellungen** *(siehe 402)*" aktivieren, um alle gemeinsam genutzten und privaten Ordner anzuzeigen. Dies gilt nur für private Ordner: Das Aktivieren dieses Kontrollkästchens verleiht dem Benutzer mit Master-Rolle genau wie dem Eigentümer sämtliche Zugriffsrechte.

Freigegebene Ordner

Die folgenden Richtlinien für **gemeinsam genutzte Ordner** gelten für Ordner unterhalb eines **gemeinsam genutzten** Cabinet:

- Untergeordnete Ordner erben die Berechtigungen des übergeordneten Ordners, es sei denn, der untergeordnete Ordner weist eigene spezifische Berechtigungen auf.
- Falls Sie die Berechtigung zum Löschen eines Ordners besitzen, werden durch Löschen dieses Ordners auch alle Objekte und Unterordner gelöscht, unabhängig von den gemeinsamen Nutzungsrechten dieser Unterordner.

  > **Hinweis:** Umfänge haben keinen Einfluss auf die Sichtbarkeit von Ordnern und Objekten in einer Ordnerstruktur. Umfänge schränken ein, womit Ihre Ordnerobjekte arbeiten können. Sie können beispielsweise gemeinsam genutzte Ordner mit Berichten, Verfahren oder Monitorsets haben, können diese Objekte jedoch nur in Rechnergruppen innerhalb Ihres Umfangs verwenden.

- Um die Nutzungsrechte zu einem Ordner einzustellen, wählen Sie den Ordner aus und klicken dann auf die Schaltfläche **Ordner gemeinsam nutzen**. Es wird das Dialogfeld **Ordner gemeinsam nutzen** angezeigt.
  - Sie können spezifische Rechte für einen Ordner mit einem einzelnen Benutzer oder einer Benutzerrolle, der/die für Sie sichtbar ist, gemeinsam nutzen. Sie haben Sichtbarkeit auf Folgendes:
    - ✓ Alle Benutzerrollen, deren Mitglied Sie sind. Dabei kommt es nicht darauf an, ob Sie diese Benutzerrolle gegenwärtig verwenden.
    - ✓ Alle einzelnen Benutzer, die Mitglieder Ihres aktuellen Umfangs sind
  - Durch Hinzufügen eines Benutzers oder einer Benutzerrolle zum **gemeinsam genutzten Feld** wird diesem Benutzer gestattet, ein beliebiges Objekt in diesem Ordner auszuführen. Dem

Benutzer bzw. der Benutzerrolle müssen keine zusätzlichen Rechte zugewiesen werden, um das Objekt auszuführen.

- Durch Markieren *zusätzlicher Rechte* wie **Bearbeiten**, **Erstellen**, **Löschen**, **Umbenennen** oder **Gemeinsam nutzen** beim Hinzufügen des Benutzers oder der Benutzerrolle werden diesem Benutzer bzw. dieser Benutzerrolle die betreffenden zusätzlichen Rechte gewährt. Sie müssen den Benutzer oder die Benutzerrolle entfernen und erneut hinzufügen, um Änderungen an den zusätzlichen Rechten vorzunehmen.
- **Gemeinsam nutzen** bedeutet, dass der Benutzer bzw. die Benutzerrolle mit dem gleichen Dialogfeld **Ordner gemeinsam nutzen**, mit dem Sie ihm gemeinsame Nutzungsrechte zugewiesen haben, auch gemeinsame Nutzungsrechte für einen ausgewählten Ordner zuweisen kann.

Verteilung

Agent-Verfahren > Verfahren verwalten > Verteilung

Die Seite **Verteilung** verteilt den Datenverkehr und die Serverlast, indem Agent-Verfahren gleichmäßig während des Tages oder eines bestimmten Zeitraums ausgeführt werden. Dies gilt für Agent-Verfahren, die gegenwärtig nur auf **periodischer Basis** ausgeführt werden.

Hinweis: Die hier aufgeführten periodischen Verfahren schließen funktionsspezifische Verfahren ein, *die nicht als Agent-Verfahren in der Ordnerstruktur Planen/Erstellen (siehe 92) sichtbar sind*, beispielsweise Verfahren, die mithilfe des Assistenten zur **Patch-Verwaltung** erstellt wurden.

Verfahren können eine übermäßige Netzwerklast verursachen, indem große Dateien zwischen Kaseya Server und Agent übertragen werden. Das gleichzeitige Ausführen dieser Vorgänge mit Hunderten von Agents kann zu einem inakzeptablen Niveau der Netzwerklast führen.

Verfahrenshistogramm

Das System plottet ein Histogramm für jedes Verfahren, das gegenwärtig für die Ausführung auf periodischer Basis geplant ist. Wenn Sie die Histogrammperiode so einstellen, dass sie dem periodischen Intervall des Verfahrens entspricht, wird gezählt, wie viele Rechner das Verfahren in einem bestimmten Zeitraum ausführen. Spitzen im Histogramm markieren visuell die Bereiche, in denen viele Rechner versuchen, das Verfahren zur selben Zeit auszuführen. *Klicken Sie auf eine Spitze, um ein Popup-Fenster mit allen Rechner-IDs anzuzeigen, die zu dieser Spitzenbelastung beitragen.* Verwenden Sie die unten aufgelisteten Steuerungen, um das Verfahren so neu zu planen, dass die Netzwerklast gleichmäßig über einen Zeitraum verteilt wird. **Nur Rechner-IDs, die gegenwärtig dem Filter für die Rechner-ID/Gruppen-ID entsprechen, werden im Histogramm gezählt.**

Gewähltes Verfahren gleichmäßig in der Histogrammperiode neu planen

Wählen Sie diese Optionsschaltfläche, um ausgewählte Verfahren neu zu planen, die auf allen Rechner-IDs ausgeführt werden, die gegenwärtig dem Filter **Rechner-ID/Gruppen-ID** *(siehe 26)* entsprechen. Die Startzeiten der Verfahrensausführung werden gleichmäßig über die gesamte Histogrammperiode verteilt.

Ausgewähltes Verfahren gleichmäßig zwischen <Startzeit> und <Endezeit> neu planen.

Wählen Sie diese Optionsschaltfläche, um ausgewählte Verfahren neu zu planen, die auf allen Rechner-IDs ausgeführt werden, die gegenwärtig dem Rechner-ID-/Gruppen-ID-Filter entsprechen. Die Startzeiten für die Verfahrensausführung werden gleichmäßig verteilt (von Startzeit bis Endzeit).

Wiederkehrend ausführen alle <N> <Perioden>

Diese Aufgabe wird immer als periodische Aufgabe ausgeführt. Geben Sie ein, wie oft diese Aufgabe in jeder Periode ausgeführt werden soll.

Überspringen, wenn Rechner offline ist

Aktivieren Sie dies, um die Aufgabe nur zur geplanten Zeit (mit einer Karenzzeit von 15 Minuten) auszuführen. Falls der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Deaktivieren Sie diese Einstellung, um diese Aufgabe auszuführen, sobald der Rechner nach der geplanten Zeit eine Verbindung herstellt.

Verteilen

Klicken Sie auf die Schaltfläche **Verteilen**, um ausgewählte Verfahren anhand der von Ihnen definierten Zeitplanparameter zu planen.

> **Hinweis:** Das periodische Verfahrensintervall wird durch die Histogrammperiode ersetzt.

Histogrammperiode auswählen

Mit dieser Option wählen Sie den Planzeitbereich für die Anzeige von Histogrammen aus.

Histogrammplots

Jedes periodisch ausgeführte Verfahren zeigt ein Histogramm aller Rechner-IDs an, auf denen dieses Verfahren während der ausgewählten Histogrammperiode ausgeführt werden soll. Nur Rechner-IDs, die gegenwärtig dem Filter für die Rechner-ID/Gruppen-ID entsprechen, werden im Histogramm gezählt.

Oberhalb des Histogramms wird Folgendes angezeigt:

- **Verfahrensname** – Name des Verfahrens. Aktivieren Sie das Kontrollkästchen neben dem Verfahrensnamen, um es zur Verteilung auszuwählen.
- **Spitze** – die höchste Anzahl von Rechnern, die das Verfahren gleichzeitig ausführen
- **Gesamt** – die Gesamtanzahl von Rechnern, auf denen das Verfahren ausgeführt wird

Skripting-Status

Agent-Verfahren > Verfahren verwalten > Agent-Verfahrensstatus

- *Auf der Registerkarte "Anstehende Verfahren" der Seiten Live Connect (siehe 393) und Rechnerübersicht (siehe 151) werden ähnliche Informationen angezeigt.*

Die Seite **Agent-Vrfahren-Status** zeigt den Status der Agent-Verfahren für eine ausgewählte Rechner-ID an. Die Liste der auswählbaren Rechner-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)*. Benutzer können auf einen Blick herausfinden, wann ein Agent-Verfahren ausgeführt wurde und ob dies erfolgreich war. Weitere Informationen über Agent-Verfahren finden Sie unter Agent-Verfahren > **Planen/Erstellen** *(siehe 92)*.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Verfahrensname

Dies ist der Name des Agent-Verfahrens.

Zeit

Dies gibt das Datum und die Uhrzeit der letzten Ausführung des Agent-Verfahrens an.

Status

Zeigt die Ergebnisse des ausgeführten Agent-Verfahrens an. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt. Wiederkehrende Agent-Verfahren werden als roter Text angezeigt.

Admin

Zeigt den VSA-Benutzer an, der das Agent-Verfahren geplant hat.

Bestätigungen ausstehend

Agent-Verfahren > Verfahren verwalten > Bestätigungen ausstehend

- Diese Seite wird nur für Benutzer mit Master-Rolle *(siehe 616)* angezeigt.

Auf der Seite **Bestätigungen ausstehend** werden *signierte* Agent-Verfahren genehmigt, sodass sie über die Seite **Planen/Erstellen** *(siehe 92)* ausgeführt oder an anderer Stelle im VSA ausgewählt und ausgeführt werden können.

Signierte Agent-Verfahren

Signierte Agent-Verfahren helfen bei der Ermittlung von nicht autorisierten Änderungen am Verfahren. *Unsignierte* Agent-Verfahren können im VSA nicht ausgeführt werden.

- Agent-Verfahren werden digital *signiert*, wenn sie von einem *beliebigen Benutzer* im Agent-Verfahren-Editor gespeichert werden.
- *Signierte* Agent-Verfahren, die von **Standardbenutzern** *(siehe 410)* erstellt werden, bedürfen der **Genehmigung** auf der Seite **Bestätigungen ausstehend**.
- Nur *Benutzer mit Master-Rolle* sind berechtigt, auf der Seite **Bestätigungen ausstehend** ausstehende signierte Agent-Verfahren zu *genehmigen*.
- Von Standardbenutzern importierte Verfahren sind zwar *signiert*, aber noch nicht *genehmigt*.

Automatisch signierte und genehmigte Agent-Verfahren

Agent-Verfahren werden automatisch signiert und genehmigt, wenn sie:

- Von Benutzern mit Master-Rolle erstellt werden
- Von Benutzern mit Master-Rolle importiert werden
- Beim Upgrade des VSA auf 7.0 in der Datenbank vorliegen

Aktionen

- **Verfahren genehmigen** – Genehmigt die ausgewählten *signierten* Agent-Verfahren.
- **Aktualisieren** – Aktualisiert die Seitenanzeige.

Tabellenspalten

- **Skriptname** – Der Name des Agent-Verfahrens

- **Geändert durch** – Der Benutzer, der die letzte Bearbeitung des Agent-Verfahrens durchgeführt hat
- **Geändert am** – Datum und Uhrzeit der letzten Änderung des Agent-Verfahrens
- **Speicherort** – Der Speicherort des Agent-Verfahrens in der Ordnerstruktur

Patch-Bereitstellung

Agent-Verfahren > Installationsassistenten > Patch-Bereitstellung

Der Assistent **Patch-Bereitstellung** ist ein Tool zum Erstellen eines Agent-Verfahrens, um Microsoft Patches zu verteilen und anzuwenden. Der Assistent leitet Sie schrittweise durch einen Prozess und Sie erhalten im Ergebnis ein Agent-Verfahren, das Sie planen können, um ein Patch auf jedem verwalteten Rechner bereitzustellen.

Microsoft gibt viele Hotfixes für bestimmte Probleme frei, die nicht im Microsoft-Update-Katalog oder Office-Erkennungstool enthalten sind. Dies sind die beiden Patch-Datenquellen, die vom **Patch-Management**-Modul verwendet werden, um Patch-Aktualisierungen zu verwalten. Mit der **Patch-Bereitstellung** können Kunden über diesen Assistenten ein Patch-Installationsverfahren für diese Hotfixes erstellen, das zur Planung der Installation auf jedem beliebigen Rechner verwendet werden kann.

Eine allgemeine Beschreibung des Patch-Managements finden Sie unter Verfahren zur Aktualisierung von Patches, Konfiguration des Patch-Managements, Patch-Verarbeitung, Abgelöste Patches, Aktualisierung der Klassifizierung und Patch-Fehler.

Schritt 1: Geben Sie eine 6-stellige Knowledge-Base-Artikelnummer ein.

Microsoft veröffentlicht umfangreiche Informationen über sein Betriebssystem in der **Microsoft Knowledge Base**. Jeder Artikel in der Knowledge-Base ist mit einer 6-stelligen Q-Nummer gekennzeichnet (z. B. Q324096). Alle Microsoft-Patches haben eine verknüpfte Knowledge-Base-Artikelnummer.

> **Hinweis:** Die Eingabe der Artikelnummer ist optional. Lassen Sie sie leer, wenn Sie sie nicht kennen.

Schritt 2: Wählen Sie die Art des Betriebssystems aus.

Manchmal gelten Patches nur für ein bestimmtes Betriebssystem. Falls das Patch, das Sie bereitstellen möchten, nur auf ein spezifisches Betriebssystem zutrifft, wählen Sie das entsprechende Betriebssystem aus der Dropdown-Liste aus. Wenn der Assistent das Verfahren zur Patch-Bereitstellung erstellt, beschränkt er die Ausführung des Verfahrens auf nur die Rechner mit dem ausgewählten Betriebssystem. Dies verhindert eine unabsichtliche Anwendung von Betriebssystem-Patches auf das falsche Betriebssystem.

Schritt 3: Laden Sie das Patch herunter.

Dieser Schritt dient nur als Erinnerung daran, das Patch von Microsoft abzurufen. Normalerweise gibt es einen Link zum Patch im Knowledge-Base-Artikel, der dieses Patch beschreibt.

Schritt 4: Wie möchten Sie das Patch anwenden?

Der Assistent zur Patch-Bereitstellung fordert Sie in Schritt 4 zur Auswahl einer Option auf: **Das Patch vom KServer an den Remote Rechner senden oder lokal ausführen** oder **Das Patch aus einer Dateifreigabe im selben LAN wie der Remote Rechner ausführen.** Das Laden des Patches auf jeden Rechner vom VSA kann sehr viel Bandbreite beanspruchen. Beim Bereitstellen eines Patches auf mehreren Rechnern in einem LAN wird keine Internetbandbreite bei der Patch-Übertragung genutzt. Jeder Rechner im LAN kann die Patch-Datei direkt von einer gemeinsamen Dateifreigabe ausführen.

Schritt 5: Wählen Sie die Patch-Datei aus oder geben Sie den UNC-Pfad zum Patch an, das im selben LAN wie der Remote Rechner gespeichert ist.

Wenn **Das Patch vom KServer an den Remote Rechner senden oder lokal ausführen** ausgewählt wurde, muss sich das Patch auf dem VSA-Server befinden. Wählen Sie die Datei aus der Dropdown-Liste aus.

> **Hinweis:** Wenn die Patch-Datei nicht in der Liste angezeigt wird, befindet sie sich nicht auf dem Kaseya Server. Klicken Sie auf die Schaltfläche **Zurück** und laden Sie die Datei auf den Kaseya Server hoch, indem Sie auf den ersten Link **hier** klicken.

Bei Auswahl von **Das Patch aus einer Dateifreigabe im selben LAN wie der Remote Rechner ausführen** muss sich das Patch vor dem Ausführen des Verfahrens zur Patch-Bereitstellung in der Remote-Dateifreigabe befinden. Der angegebene Pfad zur Datei muss im **UNC-Format** (beispielsweise `\\computername\dir\`) vorliegen.

> **Hinweis:** Wenn sich die Datei noch nicht in der Remote-Dateifreigabe befindet, können Sie sie dort über FTP ablegen. Klicken Sie auf die Schaltfläche **Zurück** und dann auf den zweiten Link **hier**. So gelangen Sie zu FTP.

Schritt 6: Geben Sie die Befehlszeilenparameter an, die zur automatischen Installation dieses Patches erforderlich sind.

Zur automatischen Bereitstellung eines Patches müssen Sie die entsprechenden Befehlszeilenparameter hinzufügen, die beim Ausführen des Patches verwendet werden. Die Parameter für eine **automatische Installation** *(siehe 616)* werden in jedem Knowledge-Base-Artikel aufgelistet. Typische Schaltereinstellungen sind `/q /m /z`.

> **Hinweis:** Befehlszeilenparameters sind optional. Lassen Sie sie leer, wenn Sie sie nicht kennen.

Schritt 7: Benennen Sie das Verfahren.

Geben Sie einen Namen für das neue Agent-Verfahren ein, das Sie zur Bereitstellung des Patches ausführen können.

Schritt 8: Starten Sie den Rechner nach dem Anwenden des Patches neu.

Aktivieren Sie dieses Kontrollkästchen, um den verwalteten Rechner nach dem Anwenden des Patches neu zu starten. Der Standardeinstellung entsprechend wird *nicht* neu gestartet.

Klicken Sie auf die Schaltfläche Erstellen.

Es wird ein neues Agent-Verfahren erstellt. Verwenden Sie Agent-Verfahren > **Planung/Erstellen** *(siehe 92)*, um das neue Agent-Verfahren in der Ordnerstruktur unter Ihrem persönlichen Ordnerbenutzernamen anzuzeigen. Sie können dieses neue Agent-Verfahren ausführen, um das Patch auf jedem verwalteten Rechner bereitzustellen.

Anwendungsbereitstellung

Agent-Verfahren > Installationsassistenten > Anwendungsbereitstellung

Mithilfe des Assistenten für die **Anwendungsbereitstellung** können Sie ein Agent-Verfahren zum Verteilen von Lieferanteninstallationspaketen erstellen. Dies ist normalerweise `setup.exe`. Der Assistent leitet Sie schrittweise durch einen Prozess und Sie erhalten im Ergebnis ein Agent-Verfahren, das Sie planen können, um eine Anwendung auf jedem verwalteten Rechner bereitzustellen.

Installationspakete von Software-Lieferanten bereitstellen

Beim Herunterladen vom Internet stellen die meisten Lieferanten eine einzige Datei bereit. Bei der Verteilung auf einer CD wird normalerweise ein Dateisatz geliefert. Durch Ausführen der Installationsdatei, normalerweise `setup.exe` oder `abc.msi`, wird die Lieferantenanwendung auf jedem beliebigen Betriebssystem installiert.

Der Assistent zur **Anwendungsbereitstellung** ermittelt die Art der Installation über ein Interview und erzeugt automatisch ein Verfahren zur Bereitstellung von Lieferanteninstallationspaketen.

Der VSA stellt ein kleines Dienstprogramm bereit, um alle unterstützten Installationstypen automatisch zu identifizieren. Laden Sie die Datei `kInstId.exe` herunter und führen Sie sie aus, um den Installationstyp automatisch zu erkennen.

> **Hinweis:** Lesen Sie den Abschnitt **Installation im Hintergrund erstellen** *(siehe 132)*, um sicherzustellen, dass die Lieferanteninstallationspakete während der Installation nicht auf eine Benutzereingabe warten.

Schritt 1: Wie möchten Sie die Anwendung bereitstellen?

Das vom Assistenten erzeugte Verfahren teilt dem verwalteten Rechner mit, wo die auszuführende Installationsdatei der Anwendung abgerufen werden muss. Der Assistent zur **Anwendungsbereitstellung** fordert Sie in Schritt 1 zur Auswahl der Installationsvorgehensweise auf: **Das Installationsprogramm vom VSA-Server an den Remote Rechner senden oder lokal ausführen** oder **Das Installationsprogramm aus einer Dateiverteilung im selben LAN wie der Remote Rechner ausführen**.

Das Laden der Installationsdatei für die Anwendung auf jeden Rechner vom VSA kann sehr viel Bandbreite beanspruchen. Beim Installieren auf mehreren Rechnern in einem LAN wird keine Internetbandbreite beansprucht, um die Installationsdatei für die Datei zu übertragen. Jeder Rechner im LAN kann diese Datei direkt von einer gemeinsamen Dateifreigabe ausführen.

Schritt 2: Wählen Sie die Anwendungsdatei für die Bereitstellung aus oder geben Sie den UNC-Pfad zum Installationsprogramm an, das im selben LAN wie der Remote Rechner gespeichert ist.

Wenn **Installationsprogramm vom VSA an den Remote Rechner senden oder lokal ausführen** ausgewählt wurde, muss sich die Installationsdatei auf dem VSA-Server befinden. Wählen Sie die Datei aus der Dropdown-Liste aus.

> **Hinweis:** Wenn die Installationsdatei nicht in der Liste angezeigt wird, befindet sie sich nicht auf dem VSA-Server. Klicken Sie auf den Link **hier**, um die Datei auf den Server hochzuladen.

Bei Auswahl von **Das Installationsprogramm aus einer Dateifreigabe im selben LAN wie der Remote Rechner ausführen** muss sich die Installationsdatei vor dem Ausführen des Verfahrens zur Anwendungsbereitstellung in der Remote Dateifreigabe befinden. Der angegebene Pfad zur Datei muss im **UNC-Format** (beispielsweise `\\computername\dir\`Stellen Sie beim Angeben eines UNC-Pfads für eine Freigabe, auf die von einem Agent-Rechner zugegriffen wird – zum Beispiel `\\machinename\share` – sicher, dass die Berechtigung der Freigabe Lese-/Schreibzugriff unter Verwendung der Anmeldedaten für diesen Agent-Rechner in > **Anmeldedaten einstellen** *(siehe 77)* zulässt.) vorliegen.

> **Hinweis:** Wenn sich die Datei noch nicht in der Remote-Dateifreigabe befindet, können Sie sie dort über FTP ablegen. Klicken Sie auf den Link **hier**, um FTP zu starten.

Schritt 3: Was ist das für ein Installationsprogramm?

Der Assistent muss wissen, welche Art von Installationsprogramm von Ihrem Softwarelieferanten zum Erstellen des Installationspakets verwendet wurde. Der VSA stellt ein kleines Dienstprogramm bereit, um alle unterstützten Installationstypen automatisch zu identifizieren. Laden Sie die Datei `kInstId.exe` herunter und führen Sie sie aus, um den Installationstyp automatisch zu erkennen.

Folgede Installationsarten werden unterstützt:

- Windows Installationsprogramm (MSI-Dateien)
- Wise Installationsprogramm
- InstallShield – Paket für das Web
- InstallShield – Mehrere Dateien
- Andere

Schritt 4: Benennen Sie das Agent-Verfahren.

Geben Sie einen Namen für das neue Agent-Vrfahren ein, das Sie zur Installation der Anwendung ausführen können.

Schritt 5: Starten Sie den Rechner nach der Installation der Anwendung neu.

Aktivieren Sie dieses Kontrollkästchen, um den verwalteten Rechner nach der Installation neu zu starten. Der Standardeinstellung entsprechend wird *nicht* neu gestartet.

Klicken Sie auf die Schaltfläche Erstellen.

Es wird ein neues Agent-Verfahren erstellt. Verwenden Sie Agent-Verfahren > **Planung/Erstellen** *(siehe 92)*, um das neue Agent-Verfahren in der Ordnerstruktur unter Ihrem persönlichen Ordnerbenutzernamen anzuzeigen. Sie können dieses neue Agent-Verfahren ausführen, um die Anwendung auf jedem verwalteten Rechner zu installieren.

Erstellen automatischer Installationen

Beim Herunterladen vom Internet stellen die meisten Lieferanten eine einzige Datei bereit. Bei der Verteilung auf einer CD wird normalerweise ein Dateisatz geliefert. Durch Ausführen der Installationsdatei, normalerweise `setup.exe`, wird die Lieferantenanwendung auf jedem beliebigen Betriebssystem installiert. Für gewöhnlich verwenden Lieferanten eine von drei Anwendungsarten, um Installationspakete zu erstellen: **InstallShield**, **Windows Installer** oder **Wise Installer**. Jede dieser Anwendungen stellt eine Methode zum Erstellen einer **automatischen Installation** *(siehe 616)* bereit. Bei einer automatischen Installation von Lieferanteninstallationspaketen müssen Sie sicherstellen, dass das Installationspaket während der Installation nicht anhält.

Automatische Installationen mit InstallShield

InstallShield verfügt über einen Aufzeichnungsmodus, der die Antworten auf alle Fragen in sämtlichen Dialogfeldern während des Installationsverfahren erfasst. Die `iis`-Datei mit den aufgezeichneten Antworten muss während der Installation auf dem verwalteten Rechner vorliegen. Zur Bereitstellung muss das Agent-Verfahren mit **writeFile()** die Dateien `setup.exe` und `record.iis` vom VSA an den verwalteten Rechner senden und dann mit **executeFile()** *(siehe 107)* die `setup.exe-Datei` mit den Optionen `/s /f"<path>\record.iis"` ausführen. Weitere Informationen über die automatische Installationsfunktion mit einer aufgezeichneten Antwortdatei finden Sie in der InstallShield-Hilfe.

Erstellen Sie ein benutzerdefiniertes Installationspaket mithilfe der folgenden Schritte:

1. Vergewissern Sie sich, dass das Installationspaket mit InstallShield erstellt wurde.
   a. Starten Sie das Installationspaket.
   b. Stellen Sie sicher, dass `InstallShield Wizard` am Ende der Fenstertitelleiste angezeigt wird.
2. Starten Sie das Installationspaket im Aufzeichnungsmodus über eine Befehlsaufforderung.
   a. **Wenn das Installationspaket aus einer einzelnen Datei besteht** – Führen Sie folgende Datei aus: `setup.exe /a /r /f1c:\temp\record.iss.`
      `Setup.exe` ist der Name des Installationspakets. `c:\temp\record.iss` ist der vollständige Pfadname zum Speichern der aufgezeichneten Ausgabe.
   b. **Wenn das Installationspaket aus mehreren Dateien besteht** – Führen Sie folgende Datei aus: `setup.exe /r /f1c:\temp\record.iss.`

`Setup.exe` ist der Name des Installationspakets. `c:\temp\record.iss` ist der vollständige Pfadname zum Speichern der aufgezeichneten Ausgabe.

3. Stellen Sie das Installationspaket mit den aufgezeichneten Dialogfeldantworten bereit. Verwenden Sie den Agent-Verfahren-Befehl **writeFile()**, um sowohl das Installationspaket des Lieferanten als auch die Datei `record.iss` auf jeden verwalteten Rechner zu kopieren oder an einen Dateiserver zu senden, auf den jeder verwaltete Rechner Zugriff hat.
4. Führen Sie das Installationspaket über den Verfahrensbefehl **executeFile()** mit den Befehlszeilenparametern für die automatische Installation aus.

a. **Wenn das Installationspaket aus einer einzelnen Datei besteht** – Führen Sie folgende Datei aus: `setup.exe /s /a /s /f1c:\temp\record.iss.`
`Setup.exe` ist der Name des Installationspakets. `c:\temp\record.iss` ist der vollständige Pfadname des Speicherorts der aufgezeichneten Einstellungen.

b. **Wenn das Installationspaket aus mehreren Dateien besteht** – Führen Sie folgende Datei aus: `setup.exe /s /f1c:\temp\record.iss.`
`Setup.exe` ist der Name des Installationspakets. `c:\temp\record.iss` ist der vollständige Pfadname des Speicherorts der aufgezeichneten Einstellungen.

Automatische Installationen mit dem Microsoft Installer

Der Windows Installer verfügt über keinen Aufzeichnungsmodus. Also kann er nur die Installationskonfiguration **Typisch** automatisch installieren. Schreiben Sie ein Verfahren, um Folgendes auszuführen und ein Windows Installer-Paket automatisch zu installieren:

1. Verwenden Sie den Agent-Verfahren-Befehl **writeFile()**, um das Installationspaket des Lieferanten auf jeden verwalteten Rechner zu kopieren oder an einen Dateiserver zu senden, auf den jeder verwaltete Rechner Zugriff hat.
2. Führen Sie das Installationspaket mit dem Parameter `/q` über den Verfahrensbefehl **executeFile()** aus.

Automatische Installationen mit dem Wise Installer

Der Wise Installer verfügt über keinen Aufzeichnungsmodus. Also kann er nur die Installationskonfiguration **Typisch** automatisch installieren. Schreiben Sie ein Verfahren, um Folgendes auszuführen und ein Wise Installer-Paket automatisch zu installieren:

1. Verwenden Sie den Agent-Verfahren-Befehl **writeFile()**, um das Installationspaket des Lieferanten auf jeden verwalteten Rechner zu kopieren oder an einen Dateiserver zu senden, auf den jeder verwaltete Rechner Zugriff hat.
2. Führen Sie das Installationspaket mit dem Parameter `/s` über den Verfahrensbefehl **executeFile()** aus.

Objekt-Manager

Agent-Verfahren > Benutzerdefinierte Installation > Packager

Der **Packager** ist ein Assistent zum Erstellen eines Pakets, wenn keine vordefinierte Installationslösung verwendet werden kann. Der **Packager** wertet den Zustand eines Quellrechners vor und nach einer Installation und/oder Änderung der Ressource aus. Der **Packager** übersetzt die Abweichungen in eine einzelne, ausführbare Datei (das **Paket**), die dann über Agent-Verfahren auf jeden verwalteten Rechner verteilt werden kann. Verteilen Sie ein Paket auf beliebige Weise. Sie können es per E-Mail senden oder auf einem Server speichern, wo ein **benutzerdefiniertes Verfahren** *(siehe 92)* eine automatische Installation auf jedem verwalteten Rechner ausführen kann.

Schritt 1: Laden Sie die Packager-Anwendung auf den Rechner herunter, auf dem der Aufbau Ihres Installationspakets geplant ist.

Um die besten Ergebnisse zu erhalten, ist es empfehlenswert, ein Paket auf einem repräsentativen

Rechner zu erstellen, also einem Rechner, der am meisten den verwalteten Rechnern entspricht, auf denen das Paket bereitgestellt wird.

Jedes Paket hängt vom Betriebssystem ab. Um es auf mehreren Betriebssystemen bereitzustellen, müssen Sie ein Paket für jedes Betriebssystem erstellen. Während der Installation überprüft der **Packager** das Betriebssystem des Zielrechners und fährt nicht fort, wenn das Paket auf einem anderen Betriebssystem als dem ursprünglichen bereitgestellt wird.

Schritt 2: Führen Sie `Packager.exe` aus und folgen Sie den Bildschirmanweisungen, um ein Verteilungspaket zu erstellen

Es werden die folgenden Aufgaben ausgeführt:

1. **Packager** erstellt einen Speicherauszug des Quellsystems.
2. Installieren Sie alle Anwendungen und/oder Ressourcen auf dem Quellsystem.
3. Führen Sie **Packager** erneut aus. **Packager** zeichnet die Änderungen im Quellsystem auf und erstellt ein Paket.

Der **Packager** nimmt vom ersten Speicherauszug an alle Vorgänge auf einem Rechner auf und erstellt das Paket. Beachten Sie bitte bei der Ausführung weiterer Aufgaben am Quellrechner, dass alle Systemänderungen in das Paket aufgenommen werden. Schließen Sie alle Anwendungen, bevor Sie den **Packager** ausführen. Dies verhindert, dass offene Anwendungen das System während der Paketerstellung abändern.

Schritt 3: Verteilen Sie das Paket über ein Skript.

Verwenden Sie Agent-Verfahren > **Planen/Erstellen** *(siehe 92)*, um ein Agent-Verfahren zum Herunterladen des Pakets auf verwaltete Rechner zu erstellen und dieses dann auszuführen. Pakete können nur auf Rechnern ausgeführt werden, auf denen Agents installiert sind. Falls die Installation des Pakets fehlschlägt, kann der **Packager** komplett erneut ausgeführt werden. Die ausführbaren Dateien zur Wiederholung und damit verknüpften Wiederherstellungsdateien befinden sich im Agent-Verzeichnis `C:\Program Files\Kaseya\KPackage` auf dem Zielrechner.

Datei abrufen

Agent-Verfahren > Dateiübertragung > Datei abrufen

Die Seite **Datei abrufen** bietet Zugriff auf Dateien, die bereits von einem verwalteten Rechner aus hochgeladen wurden. Dateien können unter Verwendung der Befehle **getFile()** oder **getFileInDirectoryPath()** in ein rechnerspezifisches Verzeichnis auf dem Kaseya Server hochgeladen werden. Wenn Sie auf die Rechner-ID klicken, werden *alle* hochgeladenen Dateien für diese Rechner-ID angezeigt. Klicken Sie auf den Link unter einer Datei, um diese Datei anzuzeigen oder auszuführen.

> **Hinweis:** Die auf dem Kaseya Server gespeicherten Dateien, die den Befehl **getFile()** verwenden, sind rechnerspezifisch. Verwenden Sie **Auf dem Server gespeicherte Dateien verwalten** *(siehe 124)* für den Zugriff auf nicht rechnerspezifische Dateien, die auf dem Kaseya Server gespeichert sind.

- Jede Datei wird als Link angezeigt. Klicken Sie auf den Dateinamen, um auf diese Datei zuzugreifen.
- Entfernen Sie Dateien, indem Sie auf das Löschsymbol ✕ neben der Datei klicken.

Beispiel 1: Gleichzeitiges Überprüfen einer großen Anzahl von verwalteten Rechnern

Datei abrufen unterstützt die gleichzeitige automatisierte Überprüfung einer großen Anzahl von verwalteten Rechnern.

> **Hinweis:** Wenn Sie einfach nur eine Datei als einmaliges Ereignis von einem verwalteten Rechner abrufen möchten, stellt "Remote Control > **FTP** *(siehe 385)*" die einfachste Methode dar.

Verwenden Sie **Datei abrufen** gemeinsam mit einem Agent-Verfahren, um einige automatisierte Aufgaben auf einer Gruppe von verwalteten Rechnern auszuführen. Wenn Sie beispielsweise über ein Dienstprogramm verfügen, das für die Clientcomputer spezifische Informationen liest, können Sie ein Verfahren schreiben, um Folgendes auszuführen:

1. Senden Sie das Dienstprogramm mithilfe des Verfahrensbefehls **writeFile()** oder der Seite **Datei verteilen** an den verwalteten Rechner.
2. Führen Sie das Dienstprogramm über den Agent-Verfahren-Befehl **executeShellCommand()** oder **executeFile()** aus und übertragen Sie die Ausgabe in eine Textdatei (z. B. `results.txt`).
3. Laden Sie die Datei mit **getFile()** auf den Kaseya Server hoch.

Beispiel 2: Vergleichen von Dateiversionen

Der Agent-Verfahren-Befehl **getFile()** bietet die Option, vorhandene Kopien von hochgeladenen Dateien vor dem nächsten Hochladen der Datei mit der Erweiterung `.bak` umzubenennen. Auf diese Weise können Sie die neueste Version und die ältere Version der Datei untersuchen. Verwenden Sie zum Beispiel den Agent-Verfahren-Editor IF-THEN-ELSE, um ein einfaches Agent-Verfahren für **getFile()** zu erstellen.

Wenn das Agent-Verfahren **getFile()** das erste Mal auf einem verwalteten Rechner ausgeführt wird, sendet der Agent die Datei `c:\temp\info.txt` an den Kaseya Server. Sie wird auf dem Kaseya Server als `news\info.txt` gespeichert. Bei der zweiten Ausführung von **getFile()** benennt der Kaseya Server das Originalexemplar von `news\info.txt` in `news\info.txt.bak` um, lädt eine neue Kopie hoch und speichert sie als `news\info.txt`.

Als Option kann auch eine E-Mail-Warnung gesendet werden, wenn eine Änderung in der hochgeladenen Datei seit ihrem letzten Hochladen ermittelt wird. Der Befehl **getFile()** muss entweder auf **Existierende Datei überschreiben und Meldung senden, wenn die Datei geändert wurde** oder **Existierende Datei speichern, Datei abrufen und Meldung senden, wenn die Datei geändert wurde** eingestellt sein.

Beispiel 3: Abrufen von Meldungen zu Dateiänderungen

Um fortlaufende Überprüfungen des Systemzustands auf verwalteten Rechnern auszuführen, führen Sie das Agent-Verfahren mit einem wiederkehrenden Zeitplan aus und aktivieren die Meldung **Dateiänderungen abrufen** unter Verwendung von Monitor > **Meldungen – Dateien abrufen** *(siehe 292)*. Der VSA benachrichtigt Sie sofort bei jeglichen Ergebnisänderungen.

Fehlerbehebung bei der Patch-Installation

Wenn in einem Patch-Scan mitgeteilt wird, dass Patch-Installationen fehlgeschlagen sind, werden die Protokolldateien `KBxxxxxx.log` (falls verfügbar) und `WindowsUpdate.log` auf den Kaseya Server hochgeladen. Außerdem wird für die Patches, die eine "Internet-basierte Installation" erforderten, die Datei `ptchdlin.xml` auf den Kaseya Server hochgeladen. Diese Dateien können unter Verwendung von Agent-Verfahren > **getFile()** *(siehe 134)* für einen bestimmten Rechner überprüft werden und bei Patch-Installationsfehlern helfen. "Infocenter > Reporting > Berichte > Protokolle > Skripting-Protokoll" enthält Einträge, die anzeigen, dass diese Protokolldateien für jeden Rechner auf den Kaseya Server hochgeladen wurden.

Datei verteilen

Agent-Verfahren > Dateiübertragung > Datei verteilen

Mit der Funktion **Datei verteilen** werden auf Ihrem VSA-Server gespeicherte Dateien an verwaltete Rechner übertragen. Sie eignet sich besonders für die Massenverteilung von Konfigurationsdateien (z. B. Virus-Footprints) oder für die Pflege der neuesten Version ausführbarer Dateien auf allen Rechnern.

Der VSA prüft die Integrität der Datei bei jedem **vollständigen Check-in** *(siehe 616)*. Sollte die Datei jemals gelöscht oder beschädigt werden oder eine aktualisierte Version davon auf dem VSA verfügbar sein, überträgt der VSA vor jeder Verfahrensausführung eine neue Kopie. Verwenden Sie diese Funktion in Verbindung mit periodischen Verfahren, um Stapelbefehle auf verwalteten Rechnern auszuführen.

> **Hinweis:** Der Verfahrensbefehl `writeFile()` führt die gleiche Aktion aus wie **Datei verteilen**. Bei jeder Ausführung des Befehls `writeFile()` prüft der Agent, ob die Datei bereits vorhanden ist oder nicht. Wenn nicht, wird die Datei erstellt. `writeFile()` ist eine bessere Methode als **Datei verteilen**, um ausführbare Dateien zu senden, die mithilfe von Agent-Verfahren auf verwalteten Rechnern ausgeführt werden sollen.

Serverdatei auswählen

Wählen Sie eine Datei aus, die an verwaltete Rechner verteilt werden soll. Dies ist derselbe Dateisatz, der durch Klicken auf den Link **Dateien verwalten...** auf dieser Seite verwaltet wird.

> **Hinweis:** Es werden nur Ihre eigenen persönlichen verwalteten Dateien oder freigegebene verwaltete Dateien angezeigt. Sollte ein anderer Benutzer eine persönliche Datei verteilen, können Sie diese nicht sehen.

Legen Sie den vollständigen Pfad und Dateinamen fest, um die Datei auf dem Remote Rechner zu speichern

Geben Sie den Pfad und Dateinamen ein, um diese Datei auf ausgewählten Rechner-IDs zu speichern.

Dateien verwalten...

Klicken Sie auf den Link **Dateien verwalten** *(siehe 124)*, um das Popup-Fenster **Auf dem Server gespeicherte Dateien verwalten** anzuzeigen. In diesem Fenster können Sie auf dem Kaseya Server gespeicherte Dateien hinzufügen, aktualisieren oder entfernen. Dasselbe Fenster wird angezeigt, wenn Sie auf die Schaltfläche **Verwaltete Dateien** in **Planen/Erstellen** *(siehe 92)* klicken. Persönliche Dateien werden mit einer dem Dateinamen vorangestellten Angabe `(Priv)` (privat) angezeigt.

Verteilen

Klicken Sie auf die Schaltfläche **Verteilen**, um die Verteilungsverwaltung der Datei zu starten, die in **Serverdatei auswählen** ausgewählt wurde und sie an den bei **Vollen Pfad und Dateinamen angeben, um Datei auf Remote Rechner zu speichern** angegebenen Speicherort zu schreiben. Dies gilt für alle markierten Rechner-IDs.

Löschen

Klicken Sie auf die Schaltfläche **Löschen**, um die Verteilung der in **Serverdatei auswählen** ausgewählten Datei von allen markierten Rechner-IDs zu entfernen.

> **Warnung:** Mit **Löschen** und **Alle löschen** wird die Datei *nicht* von verwalteten Rechnern oder dem Kaseya Server entfernt. Diese Funktionen verhindern einfach, dass die Integritätsprüfung und der Aktualisierungsprozess bei jeder vollständigen Anmeldung ausgeführt werden.

Alle löschen

Mit **Alle löschen** werden alle Dateifreigaben von allen markierten verwalteten Rechnern entfernt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Serverdatei

Dies ist der Name der Datei, die verteilt wird.

Speicherort der Agentdatei

Dies ist das Zielverzeichnis des verwalteten Rechners. Links neben jedem Zielspeicherort der Datei für eine bestimmte Rechner-ID werden zwei Symbole angezeigt. Klicken Sie auf , um die Dateifreigabe für diese Rechner-ID abzubrechen. Klicken Sie auf , um Zielpfad und Dateinamen für diese Rechner-ID zu bearbeiten.

Anwendungsprotokollierung

Agent-Verfahren > Verwaltung > Anwendungsprotokollierung

Die Seite **Anwendungsprotokollierung** enthält ein Protokoll der Aktivität des **Agent-Verfahren-Moduls** nach folgenden Kriterien:

- **Ereignis-ID**
- **Ereignisname**
- **Meldung**
- **Admin**
- **Ereignis-Datum**

Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(siehe 18, http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#6875.htm)*.

Kapitel 5

Audit

In diesem Kapitel

Inventarisierung – Überblick

Audit

Agents *(siehe 611)* können für eine automatische regelmäßige Inventarisierung der Hardware- und Softwarekonfigurationen ihrer verwalteten Rechner geplant werden. Agents geben die Informationen an den Kaseya Server zurück, sodass Sie mit dem VSA darauf zugreifen können, selbst wenn die verwalteten Rechner abgeschaltet sind. Anhand von Inventarisierungen können Sie Konfigurationen überprüfen, bevor sich diese zu ernsthaften Problemen entwickeln. Das System führt drei Arten von Inventarisierungen für jede Rechner-ID durch:

- **Referenzinventarisierung** – Die Konfiguration des Systems in seinem Originalzustand. Normalerweise wird eine Referenzinventarisierung bei der Ersteinrichtung eines Systems durchgeführt.
- **Letzte Inventarisierung** – Die Konfiguration des Systems bei der letzten Inventarisierung. Empfohlen wird einmal pro Tag.
- **Systeminformationen** – Alle DMI/SMBIOS-Daten des Systems zum Zeitpunkt der letzten Systeminformationen-Inventarisierung. Diese Daten ändern sich praktisch nie, und dieser Vorgang muss normalerweise nur einmal ausgeführt werden.

Der VSA stellt Änderungen an der Rechnerkonfiguration fest, indem er das letzte Audit mit dem Basis-Audit vergleicht. Der Datensatz der letzten Inventarisierung wird für die angegebene Anzahl von Tagen gespeichert.

Der Großteil der Daten über Agents und verwalteten Rechnern auf den Funktionsseiten und unter "Infocenter > **Berichterstellung** *(siehe 164)* > Berichte" basieren auf dem letzten Audit. Der Bericht **Rechneränderungen** stellt einen Vergleich der letzten Inventarisierung und der Referenzinventarisierung einer Rechner-ID dar. Über zwei **Alarm** *(siehe 284)*typen wird spezifisch auf die Änderungen zwischen einer Referenzinventarisierung und der letzten Inventarisierung hingewiesen: **Anwendungsänderungen** und **Hardware-Änderungen**. Die erfassten Inventarisierungsinformationen umfassen Folgendes:

- Sämtliche Hardware, einschließlich CPUs, RAM, PCI-Karten und Plattenlaufwerke.
- Gesamte installierte Software, einschließlich Lizenzen, Versionsnummern, Pfad und Beschreibung.
- Systeminformationen aus DMI und SMBIOS, einschließlich Hersteller, Modell, Seriennummer, Hauptplatinentyp des PCs sowie mehr als **40** weitere detaillierte Konfigurationsangaben.
- Betriebssysteminformationen, Versionsnummer und Service Pack.
- Aktuelle Netzwerkeinstellungen, einschließlich lokale, WAN- und Gateway-IP-Adresse, DNS-, WINS-, DHCP- und MAC-Adresse.

Funktionen	Beschreibung
Bestand anzeigen *(siehe 141)*	Bietet eine Übersicht über den gesamten, vom VSA verwalteten Bestand.
Anmeldeinformationen verwalten *(siehe 144)*	Listet die Anmeldeinformationen nach Organisation und Rechnergruppe auf.
Anmeldeinformationen-Protokolle *(siehe 146)*	Liefert ein Auditprotokoll der VSA-Benutzer, die Anmeldeinformationen erstellen, ändern und löschen.
Audit starten *(siehe 146)*	Plant letzte, System- und Referenzinventarisierungen von Rechner-IDs.
Audit-Übersicht *(siehe 149)*	Zeigt die von den Rechneraudits erfassten Daten an.
Spaltensätze konfigurieren *(siehe 150)*	Konfiguriert die Spaltensätze in der Seite "Audit-Übersicht".
Rechnerübersicht *(siehe 151)*	Zeigt detaillierte Informationen zu einem einzelnen verwalteten Rechner an.

Systeminformationen *(siehe 154)*	Zeigt die erfassten DMI/SMBIOS-Daten an.
Installierte Anwendungen *(siehe 156)*	Zeigt eine Liste der ausführbaren (.exe) Dateien auf ausgewählten verwalteten Rechnern an.
Hinzufügen/Entfernen *(siehe 157)*	Listet Programme in der Hinzufügen/Entfernen-Liste eines verwalteten Rechners auf.
Softwarelizenzen *(siehe 157)*	Zeigt eine Liste der Lizenzschlüssel an, die auf verwalteten Rechnern gefunden wurden.
Dokumente *(siehe 158)*	Speichert die mit einer Rechner-ID verknüpften Dateien.

Bestand anzeigen

Audit > Bestand > Bestand anzeigen

Die Seite "Audit > **Bestand anzeigen**" wird vom **Discovery** mit Scans von Netzwerken und Domänen gefüllt. Sie bietet eine Übersicht über den gesamten, vom VSA verwalteten Bestand. Der Bestand umfasst folgende Gerätetypen:

- **Von Agents verwaltete Rechner und Mobilgeräte** – Computer und Rechner mit installierten Agents werden automatisch als verwalteter Bestand betrachtet und auf dieser Seite aufgelistet, solange der Agent darauf installiert bleibt.
- **In den Bestand hochgestufte Geräte** – Auch wenn ein Agent auf einem erkannten Rechner nicht installiert werden kann, kann das Gerät trotzdem in den verwalteten Bestand hochgestuft und auf dieser Seite angezeigt werden. So kann ein Router oder Drucker beispielsweise auch dann überwacht werden müssen, wenn kein Agent auf dem Gerät installiert werden kann. Es gibt viele Arten von Geräte, auf denen kein Agent installiert werden kann und die aber trotzdem vom VSA überwacht werden können: Route, Switcher, Drucker, Firewalls usw. Mit der Schaltfläche **Zu Bestand machen** auf der Seite "Discovery > Ermittelte Geräte – Rasteransicht" können Geräte in den Bestand hochgestuft werden. Danach werden die betreffenden Geräte auf dieser Seite angezeigt. Hier können Sie ein Bestandsgerät über die Option **Bestand zu Gerät herabstufen** auch wieder herabstufen. Das betreffende Geräte wird von dieser Seite entfernt.

Alle verwalteten Bestandsgeräte werden einer Rechnergruppe und Organisation zugewiesen. **Scoping-Regeln** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#4578.htm)* und **Ansichtsfilter** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#214.htm)* im VSA hängen von dieser Zuweisung ab.

- Für jedes Bestandsgerät können mehrere Anmeldeinformationen definiert werden. Bei Agent-Bestandsgeräten kann ein Satz Anmeldeinformationen als Agent-Anmeldeinformationen designiert und vom **Policy Management** optional als Agent-Anmeldeinformationen verwendet werden.
- Bei Bedarf können **Service Desk**-Tickets mit den Bestandsgeräten auf dieser Seite verknüpft werden.

Aktionen

- **Anzeigen** – Öffnet ein Popup-Fenster mit den erfassten Informationen über das ausgewählte Gerät. Andere, auf dem Typ der zur Datenerfassung eingesetzten Sonde basierende Ansichten können über die Dropdown-Liste **Sondentyp** ausgewählt werden:
  - `NMAP-Sonde` – Standardmethode zur Ermittlung eines Geräts im Netzwerk mithilfe des **Discovery**-Moduls
  - `Rechner-Audit` – Audit eines Rechners mit installiertem Agent
  - `vPro` – Inventarisierung der Hardwareattribute durch ein **vPro-Audit** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#11552.htm)*

- `Gesamtansicht` – Führt alle Datenerfassungsmethoden in einer Gesamtansicht zusammen. Das ist die Standardansicht.

- **Bestand zu Gerät herabstufen** – Entfernt das ausgewählte Gerät aus dem verwalteten Bestand. Computer und Mobilegeräte mit installierten Agents können nicht herabgestuft werden.
- **Gruppe ändern** – Ändert die einem Bestandsgerät zugewiesene Organisation und Rechnergruppe.
- **Aktualisieren** – Aktualisiert die Seitenanzeige.

Tabellenspalten

- **Bestandsname** – Der Name eines Bestandsgeräts. Dies ist üblicherweise der Gerätename, kombiniert mit der VSA-Rechnergruppe und -Organisation, die dem Bestandgerät zugewiesen sind.
- **Gerätetyp** – Der Gerätetyp: Computer, Mobilgeräte, Router, Switcher, Drucker, Firewalls usw.
- **Computer-Agent** – Wenn diese Option ausgewählt ist, ist das Bestandsgerät ein Computer mit einem installierten Agent.
- **Mobil-Agent** – Wenn diese Option ausgewählt ist, ist das Bestandsgerät ein Mobilgerät mit einem installierten Agent.
- **Sonden** – Klicken Sie auf diesen Link, um die Liste der Methoden anzuzeigen, mit denen dieser Computer bzw. dieses Gerät sondiert wird.
- **Monitoring** – Wenn diese Option ausgewählt ist, wird das Bestandsgerät überwacht.
- **Patchen** – Wenn diese Option ausgewählt ist, wird das Bestandsgerät von der Patch-Verwaltung verwaltet.
- **Audit** – Wenn diese Option ausgewählt ist, wird das Bestandsgerät in regelmäßigen Abständen einem Audit unterzogen.
- **Sichern** – Wenn diese Option ausgewählt ist, wird das Bestandsgerät gesichert.
- **Sicherheit** – Wenn diese Option ausgewählt ist, ist das Bestandsgerät mit einem Virenschutz versehen.
- **Anzahl der Tickets** – Zeigt die Anzahl der offenen Tickets für dieses Bestandsgerät an.
- **Alarmzählung** – Zeigt die Anzahl von Alarmen an, die von diesem Bestandsgerät generiert werden.
- **Domain/Arbeitsgruppe** – Die Domäne oder Arbeitsgruppe, der dieses Bestandsgerät angehört (falls zutreffend)
- **SNMP aktiv** – Wenn diese Option ausgewählt ist, ist dieses Bestandsgerät SNMP-fähig.
- **vPRo aktiv** – Wenn diese Option ausgewählt ist, ist dieses Bestandsgerät vPRo-fähig.
- **Netzwerk** – Klicken Sie auf diesen Link, um die Liste der Netzwerke anzuzeigen, denen dieses Bestandsgerät angehört.
- **Gerätename** – Der Netzwerkname eines Computers oder Geräts. Wenn kein Netzwerkname vorhanden ist, wird die IP-Adresse des Geräts angezeigt.

Registerkarte Anmeldeinformationen

Hier werden die **Anmeldeinformationen** *(siehe 614)* der einzelnen Bestandsgeräte angezeigt. VSA-Benutzer können darauf zugreifen, wenn sie Zugang zu einem bestimmten Gerät oder Rechner benötigen. Optional können den einzelnen Anmeldeinformationen auch Anmerkungen hinzugefügt werden. Das Popup-Fenster **Schnellanzeige** *(siehe 17)* enthält die Option **Anmeldeinformationen anzeigen**. Der Zugriff auf die angezeigten Anmeldeinformationen über die **Schnellanzeige** kann nach Rolle und Scope eingeschränkt werden. Auf der Seite **Anmeldeinformationen verwalten** *(siehe 144)* können Sie die Anmeldeinformationen nach Organisation und Rechnergruppe festlegen.

Agent-Anmeldeinformationen

Falls es sich bei dem Bestandsgerät um einen Agent-Rechner handelt, können Anmeldeinformationen optional als **Quell-Anmeldeinformationen der Agent-Anmeldeinformationen in einer Policy Management-Richtlinie** *(http://help.kaseya.com/webhelp/DE/KPM/7000000/index.asp#8158.htm)* verwendet werden. Wenn für einen Rechner mehrere Anmeldeinformationen definiert sind, hat die lokalste Ebene Vorrang: zuerst Rechner, dann Rechnergruppe, dann Organisation. Auf jeder dieser Ebenen kann nur jeweils ein Satz

verwalteter Anmeldeinformationen als Quell-Anmeldeinformationen für die Agent-Anmeldeinformationen designiert werden.

Aktionen

- **Neu/Bearbeiten** – Legt einen Satz von Anmeldeinformationen fest.
  - **Beschreibung** – Einzeilige Beschreibung der Anmeldeinformationen
  - **Benutzername** – Der Benutzername
  - **Passwort** – Das Passwort
  - **Domäne** – Die Domäne der Anmeldeinformationen, falls vorhanden
  - **Als Agent-Anmeldeinformationen festlegen** – Nur jeweils ein Satz Anmeldeinformationen für dieses Bestandsgerät kann als Quell-Anmeldeinformationen für die Agent-Anmeldeinformationen designiert werden.
    - ✓ **Konto erstellen** – Aktivieren Sie diese Option, um auf dem verwalteten Rechner ein neues Benutzerkonto zu erstellen.
    - ✓ **Als Administrator** – Aktivieren Sie diese Option, um das neue Konto mit Administratorrechten auszustatten.
    - ✓ **Lokales Benutzerkonto** – Wählen Sie diese Option aus, um Anmeldeinformationen für eine lokale Anmeldung an diesem Rechner ohne Verweis auf eine Domäne zu verwenden.
    - ✓ **Aktuelle Domäne des Rechners verwenden** – Erstellen Sie Anmeldeinformationen unter Verwendung des Namens der Domäne, deren Mitglied dieser Rechner ist. Dies wird vom **letzten Audit** *(siehe 615)* bestimmt.
    - ✓ **Angegebene Domäne** – Verwenden Sie die oben angegebene Domäne.
  - **Anmerkungen** – Optional können den Anmeldeinformationen auch Anmerkungen hinzugefügt werden. Verwenden Sie die Werkzeugleiste, um dem Text Bilder oder eine spezielle Formatierung hinzuzufügen. *Bilder müssen hochgeladen und können nicht einfach kopiert und eingefügt werden.*



    - ✓ – Hyperlink für ausgewählten Text. Möglicherweise müssen Sie Links, die von einer anderen Quelle eingefügt wurden, zurücksetzen.
    - ✓ – Tabelle einfügen
    - ✓ – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
    - ✓ – Text einrücken
    - ✓ – Text ausrücken
    - ✓ – Formatierung entfernen
    - ✓ Ω – Symbol einfügen
    - ✓ – Emoticon einfügen
    - ✓ – Bild- und Textvorschau anzeigen
    - ✓ – Datei oder Bild hochladen
    - ✓ x_2 – Ausgewählten Text tiefgestellt festlegen
    - ✓ x^2 – Ausgewählten Text hochgestellt festlegen
    - ✓ – Vollbildmodus zur Ansicht und Bearbeitung ein- und ausschalten
- **Anzeigen** – Zeigt die Eigenschaften der ausgewählten Anmeldeinformationen an.
- **Löschen** – Löscht die ausgewählten Anmeldeinformationen.

Tabellenspalten

- **Typ** – Der Typ der Anmeldeinformationen.
  - – Dies sind Agent-Anmeldeinformationen.
  - (Leer) – Dies sind *keine* Agent-Anmeldeinformationen.
- **Name** – Der VSA-Name dieser Anmeldeinformationen.
- **Benutzername** – Der Benutzername der Anmeldeinformationen
- **Domäne** – Die Domäne der Anmeldeinformationen, falls erforderlich
- **Agent-Anmeldeinformationen** – Wenn aktiviert, sind dies die Agent-Anmeldeinformationen.
- **Konto erstellen** – Erstellt das Konto, falls es noch nicht vorhanden ist.
- **Als Administrator** – Das Konto wird mit Administratorrechten erstellt.

Registerkarte "vPro"

Audit > Bestand anzeigen > Registerkarte "vPro"

Die Registerkarte "Audit > Bestand anzeigen > **vPro**" zeigt Hardwaredaten über vPro-fähige Rechner an, die erkannt werden, indem im Dialogfeld Netzwerk bearbeiten ein vPro-Scan aktiviert und ausschließlich LAN-Watch ausgeführt wird. Diese Informationen sind nur verfügbar, wenn die vPro-Anmeldeinformationen eines Rechners von **LAN-Watch** angegeben werden.

Vom vPro-Rechner ausgegebenen Hardwaredaten können wie folgt sein:

- Status der Agent-Anmeldung, falls ein Agent auf dem vPro-Rechner installiert ist
- Rechnerinformationen
- Motherboard-Bestandsinformationen
- BIOS-Daten
- Prozessorinformationen
- RAM-Informationen
- Festplatteninformationen

Hinweis: Das **Desktop Policy**-Modul bietet **Funktionen für das vPro-Management** *(http://help.kaseya.com/webhelp/DE/KDPM-Online-Help.asp?10070.htm)*.

Intel vPro Rebate: Kaseya nimmt an einem von Intel angebotenen vPro-Rebate-Programm teil. Wenn Sie vPro-fähige Rechner installiert haben und LAN-Watch ausführen (und der vPro-Rechner für das Rebate geeignet ist), können Sie schnell die benötigten Informationen erzeugen, indem Sie auf die Schaltfläche **Intel® vPro™-Rebate-Datei generieren** klicken. Dies erzeugt eine .CVS-Datei mit den Informationen, die Sie zum Dokumentieren Ihres Rebate-Anspruchs mit Intel benötigen. Außerdem wird der Link **Intel® vPro™ Technology Activation Rebate-Regeln** bereitgestellt.

Anmeldeinformationen verwalten

Audit > Bestand > Anmeldeinformationen verwalten

Auf der Seite **Anmeldeinformationen verwalten** werden **Anmeldeinformationen** *(siehe 614)* nach Organisation und Rechnergruppe angegeben. VSA-Benutzer können darauf zugreifen, wenn sie Zugang zu einem bestimmten Gerät oder Rechner benötigen. Optional können den einzelnen Anmeldeinformationen auch Anmerkungen hinzugefügt werden.

Anmeldeinformationen in der Schnellanzeige

Das Popup-Fenster **Schnellanzeige** *(siehe 17)* enthält die Option **Anmeldeinformationen anzeigen**. Der Zugriff auf die angezeigten Anmeldeinformationen über die **Schnellanzeige** kann nach Rolle und Scope

eingeschränkt werden. Anmeldeinformationen nach einzelnen Rechnern oder Geräten legen Sie auf der Seite **Bestand anzeigen** *(siehe 141)* fest.

Agent-Anmeldeinformationen

Falls es sich bei dem Bestandsgerät um einen Agent-Rechner handelt, können Anmeldeinformationen optional als **Quell-Anmeldeinformationen der Agent-Anmeldeinformationen in einer Policy Management-Richtlinie** *(http://help.kaseya.com/webhelp/DE/KPM/7000000/index.asp#8158.htm)* verwendet werden. Wenn für einen Rechner mehrere Anmeldeinformationen definiert sind, hat die lokalste Ebene Vorrang: zuerst Rechner, dann Rechnergruppe, dann Organisation. Auf jeder dieser Ebenen kann nur jeweils ein Satz verwalteter Anmeldeinformationen als Quell-Anmeldeinformationen für die Agent-Anmeldeinformationen designiert werden. Verwaltete Anmeldeinformationen werden erstellt, wenn ein Benutzer den **Systems Management ConfigurationEinrichtungsassistenten** *(http://help.kaseya.com/webhelp/DE/KDPM/7000000/index.asp#10070.htm)* für eine Organisation ausführt.

Spalten im mittleren Feld

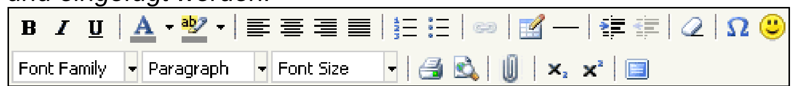
Die Zeilen sind zunächst nach Organisation, dann nach Rechnergruppe und schließlich nach Rechner-ID sortiert.

- **(Stufe)** – Weist die Zeile als Organisation , Rechnergruppe oder Rechner-ID aus.
- **Name** – Der Name der Organisation, Rechnergruppe oder Rechner-ID
- **Anmeldeinformationen** – Zeigt einen Schlüssel an, wenn für diese Zeile mindestens ein Satz Anmeldeinformationen definiert ist.

Aktionen im rechten Feld

Wählen Sie vor der Durchführung dieser Aktionen eine Organisation oder Rechnergruppe aus.

- **Neu/Bearbeiten** – Legt einen Satz von Anmeldeinformationen fest.
  - **Beschreibung** – Einzeilige Beschreibung der Anmeldeinformationen
  - **Benutzername** – Der Benutzername
  - **Passwort** – Das Passwort
  - **Domäne** – Die Domäne der Anmeldeinformationen, falls vorhanden
  - **Als Agent-Anmeldeinformationen festlegen** – Nur jeweils ein Satz Anmeldeinformationen für diese Organisation oder Rechnergruppe kann als Quell-Anmeldeinformationen für die Agent-Anmeldeinformationen designiert werden.
    - ✓ **Konto erstellen** – Aktivieren Sie diese Option, um auf dem verwalteten Rechner ein neues Benutzerkonto zu erstellen.
    - ✓ **Als Administrator** – Aktivieren Sie diese Option, um das neue Konto mit Administratorrechten auszustatten.
    - ✓ **Lokales Benutzerkonto** – Wählen Sie diese Option aus, um Anmeldeinformationen für eine lokale Anmeldung an diesem Rechner ohne Verweis auf eine Domäne zu verwenden.
    - ✓ **Aktuelle Domäne des Rechners verwenden** – Erstellen Sie Anmeldeinformationen unter Verwendung des Namens der Domäne, deren Mitglied dieser Rechner ist. Dies wird vom **letzten Audit** *(siehe 615)* bestimmt.
    - ✓ **Angegebene Domäne** – Verwenden Sie die oben angegebene Domäne.
  - **Anmerkungen** – Optional können den Anmeldeinformationen auch Anmerkungen hinzugefügt werden. Verwenden Sie die Werkzeugleiste, um dem Text Bilder oder eine spezielle Formatierung hinzuzufügen. *Bilder müssen hochgeladen und können nicht einfach kopiert und eingefügt werden.*



    - ✓ – Hyperlink für ausgewählten Text. Möglicherweise müssen Sie Links, die von einer anderen Quelle eingefügt wurden, zurücksetzen.

- ✓ – Tabelle einfügen
- ✓ — – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
- ✓ – Text einrücken
- ✓ – Text ausrücken
- ✓ – Formatierung entfernen
- ✓ Ω – Symbol einfügen
- ✓ – Emoticon einfügen
- ✓ – Bild- und Textvorschau anzeigen
- ✓ – Datei oder Bild hochladen
- ✓ x_2 – Ausgewählten Text tiefgestellt festlegen
- ✓ x^2 – Ausgewählten Text hochgestellt festlegen
- ✓ – Vollbildmodus zur Ansicht und Bearbeitung ein- und ausschalten

- **Löschen** – Löscht die ausgewählten Anmeldeinformationen.

Tabellenspalten

- **Benutzername** – Der Benutzername der Anmeldeinformationen
- **Passwort** – Das Passwort der Anmeldeinformationen
- **Domäne** – Die Domäne der Anmeldeinformationen, falls zutreffend
- **Geerbt von** – Die Stufe, aus der die Anmeldeinformationen geerbt werden. Anmeldeinformationen können aus einer höherstufigen Organisation oder Rechnergruppe geerbt werden.
- **Agent** – Wenn aktiviert, sind dies die Agent-Anmeldeinformationen.
- **Beschreibung** – Der VSA-Name der Anmeldeinformationen
- **Anmerkungen** – Anmerkungen zu den Anmeldeinformationen

Anmeldeinformationen-Protokolle

Audit > Bestand > Anmeldeinformationen-Protokolle

Die Seite **Anmeldeinformationen-Protokolle** liefert ein Auditprotokoll der VSA-Benutzer, die auf den Seiten **Bestand anzeigen** *(siehe 141)* und **Anmeldeinformationen verwalten** *(siehe 144)* Anmeldeinformationen erstellen, ändern und löschen.

- **Ereignis-ID**
- **Ereignisname**
- **Meldung**
- **Admin**
- **Ereignis-Datum**

Audit starten

Audit > Daten sammeln > Audit starten

Über die Seite **Inventarisierung ausführen** wird eine Inventarisierung der Hardware- und Softwarekonfiguration von verwalteten Rechnern ausgeführt.

Inventarisierungen

Agents *(siehe 611)* können für eine automatische regelmäßige Inventarisierung der Hardware- und Softwarekonfigurationen ihrer verwalteten Rechner geplant werden. Agents geben die Informationen

an den Kaseya Server zurück, sodass Sie mit dem VSA darauf zugreifen können, selbst wenn die verwalteten Rechner abgeschaltet sind. Anhand von Inventarisierungen können Sie Konfigurationen überprüfen, bevor sich diese zu ernsthaften Problemen entwickeln. Das System führt drei Arten von Inventarisierungen für jede Rechner-ID durch:

- **Referenzinventarisierung** – Die Konfiguration des Systems in seinem Originalzustand. Normalerweise wird eine Referenzinventarisierung bei der Ersteinrichtung eines Systems durchgeführt.
- **Letzte Inventarisierung** – Die Konfiguration des Systems bei der letzten Inventarisierung. Empfohlen wird einmal pro Tag.
- **Systeminformationen** – Alle DMI/SMBIOS-Daten des Systems zum Zeitpunkt der letzten Systeminformationen-Inventarisierung. Diese Daten ändern sich praktisch nie, und dieser Vorgang muss normalerweise nur einmal ausgeführt werden.

Der VSA stellt Änderungen an der Rechnerkonfiguration fest, indem er das letzte Audit mit dem Basis-Audit vergleicht. Der Datensatz der letzten Inventarisierung wird für die angegebene Anzahl von Tagen gespeichert.

Der Großteil der Daten über Agents und verwalteten Rechnern auf den Funktionsseiten und unter "Infocenter > **Berichterstellung** *(siehe 164)* > Berichte" basieren auf dem letzten Audit. Der Bericht **Rechneränderungen** stellt einen Vergleich der letzten Inventarisierung und der Referenzinventarisierung einer Rechner-ID dar. Über zwei **Alarm** *(siehe 284)*typen wird spezifisch auf die Änderungen zwischen einer Referenzinventarisierung und der letzten Inventarisierung hingewiesen: **Anwendungsänderungen** und **Hardware-Änderungen**.

Aktionen

- **Ein Audit planen** – Klicken Sie auf **Ein Audit planen** oder **Audit neu planen**, um das Fenster **Scheduler** zu öffnen, das im gesamten VSA zur Planung von Aufgaben verwendet wird. Planen Sie die einmalige oder periodische Ausführung einer Aufgabe. Jede Art der Wiederholung (einmal, stündlich, täglich, wöchentlich, monatlich, jährlich) zeigt weitere Optionen für diese Art der Wiederholung an. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. *Nicht alle Optionen stehen für jede geplante Aufgabe zur Verfügung.* Optionen können Folgendes umfassen:
  - **Basis-Audit**, **Aktuelles Audit** oder **Systeminformationen** – Audittyp.
  - **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > Einstellungen" festgelegt ist.   Übernimmt die Standardeinstellungen aus der Seite "System > Standardeinstellungen".
  - **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.
  - **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
  - **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
  - **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.

- **Audit neu planen** – Füllt den Scheduler mit den Daten eines ausstehenden Audits, damit Sie Anpassungen vornehmen können.
- **Audit jetzt ausführen** – Plant das Audit zur sofortigen Ausführung.
- **Audit abbrechen** – Bricht ein geplantes Audit ab.

Erinnere mich, wenn für Konten eine Inventarisierung geplant werden muss

Wenn diese Option aktiviert ist, wird eine Warnmeldung anzeigt, wenn für eine oder mehrere Rechner-IDs keine Inventarisierungen geplant sind. Diese Warnung wird bei jedem Auswählen von **Inventarisierung ausführen** angezeigt. Trifft auf jeden einzelnen VSA-Benutzer zu.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Rechner.Gruppen-ID

Auf der ersten Zeile wird die Rechner-ID angegeben. Auf der letzten Zeile wird die Uhrzeit angegeben, zu der die letzte Inventarisierung der Systeminformationen durchgeführt wurde. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt. Datum-/Zeitstempel für überfällige und abgeschlossene Vorgänge werden als schwarzer Text angezeigt.

Systeminformationen / Aktuelles Audit / Basis-Audit

Die Spalten geben an, wann der betreffende Audit-Typ zuletzt durchgeführt wurde. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt.Datum-/Zeitstempel für überfällige und abgeschlossene Vorgänge werden als schwarzer Text angezeigt.

Nächstes Audit

Zeigt an, wann die nächste letzte Inventarisierung geplant ist. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt.Datum-/Zeitstempel für überfällige und abgeschlossene Vorgänge werden als schwarzer Text angezeigt.

Wiederkehrendes Intervall

Zeigt das periodische Intervall für aktuelle Audits an.

Audit-Übersicht

Audit > Gruppendaten anzeigen > Audit-Übersicht

Die Seite "Audit > **Audit-Übersicht**" bietet einen Überblick über die von Audits über die Seite **Audit starten** *(siehe 146)* erfassten Rechnerdaten. Die Spalten der Auditdaten auf dieser Seite können individuell ausgewählt und gefiltert werden. Auch benutzerdefinierte Spaltensätze können ausgewählt werden. Spaltensätze werden im Vorhinein auf der Seite **Spaltensätze konfigurieren** *(siehe 150)* definiert. Zusätzliche Daten, die nicht auf der Seite **Audit-Übersicht** verfügbar sind, können auf der Seite **Rechnerübersicht** *(siehe 151)* eingesehen werden. Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(siehe 18)*.

Die Seite umfasst die folgenden Spalten von Auditdaten (in der standardmäßigen Reihenfolge):

- **Rechner-ID** – Der Name, der den Rechner innerhalb des VSA ausweist. Beruht üblicherweise auf dem Computernamen.
- **Aktueller Benutzer** – Anmeldename des gegebenenfalls aktuell am Rechner angemeldeten Benutzers
- **Letzter Neustartzeitpunkt** – Zeitpunkt des zuletzt bekannten Zeitpunkts des Rechnerneustarts
- **Letzter Check-in-Zeitpunkt** – Der letzte Zeitpunkt, an dem ein Rechner beim Kaseya Server eingecheckt wurde
- **Gruppen-ID** – Gruppen-ID-Teil der Rechner-ID
- **Erster Check-in-Zeitpunkt** – Der Zeitpunkt, an dem ein Rechner zum ersten Mal beim Kaseya Server eingecheckt wurde
- **Zeitzone** – Vom Rechner verwendete Zeitzone
- **Rechnername** – Der Name, der dem Rechner von seinen Benutzern zugewiesen wurde
- **Domäne/Arbeitsgruppe** – Arbeitsgruppe oder Domäne, zu der der Rechner gehört.
- **DNS-Computername** – Der voll qualifizierte DNS-Computername, mit dem der Rechner im Netzwerk identifiziert wird. Besteht üblicherweise aus Rechnernamen und Domänennamen. Zum Beispiel: `jsmithxp.acme.com`. Wenn der Rechner zu einer Arbeitsgruppe gehört, wird nur der Rechnername angezeigt.
- **Betriebssystem** – Typ des Betriebssystems, das auf dem Rechner ausgeführt wird
- **BS-Version** – Versionsreihe des Betriebssystems.
- **CPU-Typ** – Prozessorversion und -modell.
- **CPU-Geschwindigkeit** – Taktgeschwindigkeit des Prozessors.
- **Prozessorzahl** – Anzahl der Prozessoren.
- **RAM (MB)** – Arbeitsspeicher des Rechners
- **Agent-Version** – Versionsnummer des auf dem Rechner geladenen Kaseya-Agents.
- **Letzter angemeldeter Benutzer** – Anmeldename des zuletzt am Rechner angemeldeten Benutzers.
- **Primärer/Sekundärer KServer** – Vom Rechner verwendete IP-Adresse und Name zur Kommunikation mit dem Kaseya Server
- **Intervall für Schnellanmeldung** – Zeiteinstellung für **Schnellanmeldung** *(siehe 616)* in Sekunden.
- **Kontaktname** – Unter **Profil bearbeiten** *(siehe 73)* eingegebener Rechnerbenutzername.
- **Kontakt-E-Mail** – E-Mail-Adresse wie in "Profil bearbeiten" eingegeben.
- **Kontakt-Telefon** – In "Profil bearbeiten" eingegebene Telefonnummer.
- **Hersteller** – Systemhersteller.
- **Produktname** – Produktname des Systems.
- **Systemversion** – Versionsnummer des Produkts.
- **System-Seriennummer** – Seriennummer des Systems.
- **Gehäuse-Seriennummer** – Seriennummer auf dem Gehäuse.
- **Gehäuse-Bestandsetikett** – Bestandsetikett auf dem Gehäuse.
- **Externe Busgeschwindigkeit** – Busgeschwindigkeit des Motherboards.

- **Max. Speichergröße** – Maximale Speichergröße des Motherboards.
- **Max. Speichersteckplätze** – Gesamtzahl der verfügbaren Speichermodulsteckplätze.
- **Gehäusehersteller** – Hersteller des Gehäuses.
- **Gehäusetyp** – Typ des Gehäuses.
- **Gehäuseversion** – Versionsnummer des Gehäuses.
- **Motherboard-Hersteller** – Hersteller des Motherboards.
- **Motherboard-Produkt-ID** – Produkt-ID des Motherboards
- **Motherboard-Version** – Versionsnummer des Motherboards.
- **Motherboard-Seriennummer** – Seriennummer des Motherboards.
- **Prozessorfamilie** – Installierter Prozessortyp.
- **Prozessorhersteller** – Hersteller des Prozessors.
- **Prozessorversion** – Versions-ID des Prozessors.
- **Max. CPU-Geschwindigkeit** – Maximal unterstützte Prozessorgeschwindigkeit.
- **Aktuelle CPU-Geschwindigkeit** – Aktuelle Geschwindigkeit des Prozessors
- **IPv6 Adresse** – Dem Rechner zugewiesene IP-Adresse im Format Version 4
- **IPv6 Adresse** – Dem Rechner zugewiesene IP-Adresse im Format Version 6.
- **Subnetz-Maske** – Dem Rechner zugewiesenes Netzwerksubnetz.
- **Standard-Gateway** – Dem Rechner zugewiesener Standard-Gateway.
- **Verbindungs-Gateway** – Die vom Kaseya Server erkannte IP-Adresse, wenn dieser Rechner eingecheckt wird. Befindet sich der Rechner hinter einem DHCP-Server, ist dies die öffentliche IP-Adresse des Subnetzes.
- **Land** – Mit dem Connection-Gateway verknüpftes Land.
- **MAC-Adresse** – MAC-Adresse der LAN-Karte, die zur Kommunikation mit dem Kaseya Server verwendet wird
- **DNS-Server** – IP-Adresse des dem Rechner zugewiesenen DNS-Servers
- **DHCP-Server** – IP-Adresse des von diesem Rechner verwendeten DHCP-Servers.
- **Primärer/Sekundärer WINS** – WINS-Einstellungen.
- **Freier Speicherplatz** – Der freie Datenspeicherplatz in GB
- **Freier Speicherplatz** – Der belegte Datenspeicherplatz in GB
- **Gesamtgröße** – Der gesamte Datenspeicherplatz in GB
- **Anzahl der Laufwerke** – Die Anzahl der Laufwerke auf dem Rechner
- **Portalzugriffsanmeldung** – Der einem Benutzer zur Anmeldung beim Kaseya Server zugewiesene Anmeldename
- **Portalzugriff-Fernsteuerung** – Dies ist aktiviert, wenn sich dieser Rechnerbenutzer anmelden und die Fernsteuerung *zu seinem eigenen Rechner von einem anderen Rechner aus* aktivieren kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Portalzugriff-Ticketing** – Dies ist aktiviert, wenn sich dieser Rechnerbenutzer anmelden und Tickets eingeben kann. Deaktiviert, wenn der Zugriff verweigert wurde.
- **Portalzugriff-Chat** – Dies ist aktiviert, wenn dieser Rechnerbenutzer Chat-Sitzungen mit einem VSA-Benutzer *einleiten* darf. Deaktiviert, wenn der Zugriff verweigert wurde.

Spaltensätze konfigurieren

Audit > Gruppendaten anzeigen > Spaltensätze konfigurieren

Auf der Seite **Spaltensätze konfigurieren** werden Spaltensätze konfiguriert, die anschließend in der Tabelle "Audit > **Audit-Übersicht** *(siehe 149)*" ausgewählt werden können.

Aktionen

- **Neu** – Erstellt einen neuen Spaltensatz.
- **Bearbeiten** – Bearbeitet einen ausgewählten Spaltensatz.
- **Löschen** – Löscht einen ausgewählten Spaltensatz.

Spaltensatz auswählen

Wählen Sie im mittleren Feld dieser Seite einen bestehenden Spaltensatz aus. Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen < und >, um die vorherige und nächste Seite anzuzeigen. In der Dropdown-Liste wird der erste Datensatz jeder Seite mit Daten in der *Sortierreihenfolge der ausgewählten Spalte auf dieser Seite* angezeigt.

Rechnerübersicht

Audit > Individuelle Daten anzeigen > Rechnerübersicht

- Ähnliche Informationen werden auch unter "Infocenter > Berichterstellung > Rechnerübersicht *(siehe 207)*" angezeigt.

Rechnerübersicht

Über die Seite **Rechnerübersicht** können Benutzer Aufgaben und Funktionen für jeweils nur einen verwalteten Rechner ausführen. Eine Reihe von Eigenschaftenblättern in Form von Registerkarten ermöglicht den Zugriff auf verschiedene Kategorien von Informationen zu dem verwalteten Rechner.

Aktionen

Es kann vorkommen, dass Sie benutzerdefinierte Feldwerte oder auch die bei einem Systemaudit erfassten Daten eines Rechners bearbeiten möchten. Bearbeitungen der Auditdaten werden von nachfolgenden Systemaudits überschrieben, es sei denn, Sie entfernen die betreffenden Systemauditfelder aus der automatischen Erfassung. Bearbeitete Systemauditfelder und benutzerdefinierte Felder können auf der Seite "Agent > **Agent-Status** *(siehe 32)*" auf der Seite **Zusammengeführte Tabelle filtern** *(siehe 30)* und im Bericht **Gesamttabelle** *(siehe 206)* ausgewählt werden. Sie können die Änderungen der Werte von Datenelementen auch automatisieren, indem Sie den Befehl **updateSystemInfo()** *(siehe 117)* in einem Agent-Verfahren ausführen.

- **Rechnerdaten bearbeiten** – Bearbeitet die bei einem Systemaudit erfassten Daten eines Rechners. Die Werte in benutzerdefinierten Feldern können ebenfalls geändert werden.
- **Automatische Sammlung bearbeiten** – Heben Sie die Markierung einzelner Elemente auf, um sie vor Überschreibung durch nachfolgende Systemaudits zu schützen. Diese Optionen werden zusammen mit dem Dialogfeld **Rechnerdaten bearbeiten** verwendet.
- **Massenbearbeitung, benutzerdefiniert** – Ändert die Werte in benutzerdefinierten Feldern auf mehreren Rechnern.
  1. Wählen Sie mehrere Rechnerzeilen aus.
  2. Klicken Sie auf **Massenbearbeitung, benutzerdefiniert**.
  3. Wählen Sie in der Dropdown-Liste **Benutzerdefiniertes änderbares Feld** ein benutzerdefiniertes Feld aus.
  4. Ersetzen Sie den vorhandenen Wert, indem Sie:
     - ✓ Einen vorhandenen Ersatzwert aus der Dropdown-Liste auswählen ODER
     - ✓ Den Ersatzwert manuell eingeben.

Sie können eine unbegrenzte Anzahl von benutzerdefinierten Feldern mit Informationen über verwaltete Rechner pflegen. Dies erfolgt sowohl auf der Registerkarte **Zusammenfassung** als auch auf der Registerkarte "Hardware > **Zusammenfassung**" auf dieser Seite sowie auf der Seite "Audit > **Systeminformationen** *(siehe 154)*". Benutzerdefinierte Felder werden in Ansichten, Verfahren und

Berichten unterstützt. Benutzerdefinierte Berichte können jedoch höchstens 40 benutzerdefinierte Felder aufnehmen.

- **Neues benutzerdefiniertes Feld** – Erstellt ein neues benutzerdefiniertes Feld.
- **Benutzerdefiniertes Feld umbenennen** – Benennt ein benutzerdefiniertes Feld um.
- **Benutzerdefiniertes Feld löschen** – Löscht ein benutzerdefiniertes Feld.

Einen Rechner auswählen

Wählen Sie im mittleren Feld einen Rechner aus, um Informationen darüber anzuzeigen. Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen < und >, um die vorherige und nächste Seite anzuzeigen. In der Dropdown-Liste wird der erste Datensatz jeder Seite mit Daten in der *Sortierreihenfolge der ausgewählten Spalte auf dieser Seite* angezeigt.

Übersicht

- **Sammlungen** – Zeigt die **Sammlungen** *(siehe 628)*, denen der Rechner zugehörig ist. Dies wird über die Option **Nur ausgewählte Rechner-IDs zeigen** in **Ansichtsdefinitionen** *(siehe 27)* definiert.
- **Name/Betriebssystem-Daten** – Zeigt Name, Betriebssystem und Betriebssystemversion an.
- **Systeminformationen** – Zeigt Systemhersteller, Produktname, Version und Seriennummer an.
- **Netzwerkinformationen** – Zeigt die Netzwerkkonfigurationseinstellungen an.
- **CPU/RAM-Daten** – Zeigt die technischen Daten für Prozessor und Arbeitsspeicher an.
- **Benutzerdefinierte Felder** – Zeigt benutzerdefinierte Felder und Werte an, die vom Benutzer dieses Rechners zugewiesen wurden.

Software

- **Systeminformationen** – Listet die Hardwareattribute und zugehörige Informationen auf.
- **Softwarelizenzen** – Listet alle Softwarelizenzen auf, die für eine ausgewählte Rechner-ID ermittelt wurden. Doppelte Lizenzschlüssel, die auf mehr als einem Rechner gefunden werden, werden als roter Text angezeigt. Durch Klicken auf den Nummern-Link neben dem Titel einer doppelten Lizenz werden die Rechner-IDs aufgelistet, die die doppelte Lizenz verwenden.
- **Installierte Anwendungen** – Listet die auf dem verwalteten Rechner installierten Anwendungen auf.
- **Hinzufügen/Entfernen** – Zeigt die Programme an, die im Fenster "Programme" auf Windows-Rechnern aufgelistet sind.
- **Anw. starten** – Zeigt die Programme an, die bei der Anmeldung des Benutzers automatisch gestartet werden.
- **Sicherheitsprodukte** – Bezeichnet den Installationsstatus der Virenschutzprodukte, die im *Windows-Sicherheitscenter* von Windows-Rechnern registriert sind. Ab Windows 7 trägt das *Windows-Sicherheitscenter* den Namen *Wartungscenter*.

Hardware

- **Übersicht**
  - **Systeminformationen** – Listet die Hardwareattribute und zugehörige Informationen auf.
  - **Netzwerkinformationen** – Zeigt die Netzwerkkonfigurationseinstellungen an.
  - **Gehäuse** – Zeigt Hersteller, Typ, Version, Seriennummer und Bestandsetikett des Gehäuses an.
  - **Hauptplatine** – Zeigt Hersteller, Produkt, Version, Seriennummer und externe Busgeschwindigkeit der Hauptplatine an.
  - **CPU/RAM-Daten** – Zeigt die technischen Daten für Prozessor und Arbeitsspeicher an.
  - **Benutzerdefinierte Felder** – Zeigt benutzerdefinierte Felder und Werte an, die vom Benutzer dieses Rechners zugewiesen wurden.
- **Drucker** – Listet die Drucker und Ports auf, an die ein Rechner Druckaufträge senden kann.

- **PCI & Disk-Hardware** – Zeigt Typ, Hersteller und Produktnamen an.
- **Platten-Datenträger** – Zeigt Informationen zu Platten-Datenträgern an.
- **Festplattenpartitionen** – Zeigt die Partitionen in allen Datenträgern an.
- **Datenträgerfreigaben** – Zeigt die freigegebenen Ordner an.

Agent

- **Einstellungen** – Zeigt Informationen über den Agent auf dem verwalteten Rechner an:
  - **Agentversion**
  - **Aktueller Benutzer**
  - **Letzter Check-in**
  - **Letzter Neustart**
  - **Erster Check-in**
  - **Zugehörigkeit zu Patch-Richtlinie** – Wird definiert unter Patch-Verwaltung > Mitgliedschaft: Patch-Richtlinie.
  - **Definitionskollektionen anzeigen** – Wird über die Option **Nur ausgewählte Rechner-IDs anzeigen** in **Ansichtsdefinitionen** *(siehe 27)* definiert.
  - **Arbeitsverzeichnis** – Kann auch über "Agent > **Arbeitsverzeichnis** *(siehe 72)*" definiert werden.
  - **Check-in-Kontrolle** – Kann auch über "Agent > **Check-in-Kontrolle** *(siehe 68)*" definiert werden.
  - **Profil bearbeiten** – Kann auch über "Agent > **Profil bearbeiten** *(siehe 73)*" definiert werden.
  - **Agent-Protokolle und Profile** – Kann auch über "Agent > **Protokollhistorie** *(siehe 36)*" definiert werden.
- **Protokolle** – Zeigt die für diesen Rechner verfügbaren Protokolle an: Alarmprotokoll, Monitoraktionsprotokoll, Agent-Protokoll, Konfigurationsänderungen, Netzwerkstatistiken, Ereignisprotokoll, Agent-Verfahrensprotokoll, Fernsteuerungsprotokoll, Protokoll-Monitoring.
  - **Anstehende Verfahren** – Zeigt anstehende Verfahren und die Verfahrenshistorie für einen verwalteten Rechner an. einschließlich des Datums/der Uhrzeit/des Status der Ausführung und des Benutzers, der das Verfahren plante.

Meldungen

- Definiert Meldungen für einen Rechner: **Agent-Status** *(siehe 286)*, **Anwendungsstatus** *(siehe 289)*, **Datei-Änderungen abrufen** *(siehe 292)*, **Hardware-Änderungen** *(siehe 295)*, **Geringer Speicherplatz** *(siehe 297)*, LAN-Watch, **Fehlschlagen des Agent-Verfahrens** *(siehe 299)*, **Schutzverletzungen** *(siehe 302)*, **Patch-Meldung** *(siehe 306)*, **Backup-Meldung** *(siehe 310)*.

Patch-Status

- Zeigt `fehlende` und `ausstehende` Microsoft-Patches an und plant fehlende Patches. Wenn ein Rechner zu einer **Patch-Richtlinie** *(siehe 624)* gehört, können fehlende Patches außerdem auch als `Denied (Pending Approval)` identifiziert werden. Der Benutzer kann die Patch-Richtlinie "Abgelehnt" manuell außer Kraft setzen, indem er das Patch plant.
  - Klicken Sie auf die Schaltfläche **Planen**, um ein ausgewähltes fehlendes Patch zu planen.
  - Klicken Sie auf die Schaltfläche **Abbrechen**, um ein ausgewähltes anstehendes Patch zu stornieren.
  - Klicken Sie auf den Link **Historie anzeigen**, um die Historie der auf dem verwalteten Rechner installierten Patches anzuzeigen.

Remote Control

- Zeigt den Status von Remote-Control-Sitzungen auf dem verwalteten Rechner an: Remote Control, FTP und Chat. VSA-Benutzer können festlegen, welches Remote-Control-Paket bei der Remote-Control-Sitzung eingesetzt werden soll.

Dokumente

- Listet die Dokumente auf, die für einen verwalteten Rechner auf den Kaseya Server hochgeladen wurden. Sie können zusätzliche Dokumente hochladen. Dies stellt dieselbe Funktionalität wie "Audit > **Dokumente** *(siehe 158)*" bereit.

Benutzer

- **Konten** – Listet alle Benutzerkonten für verwaltete Rechner auf.
- **Gruppen** – Listet alle Benutzergruppen für verwaltete Rechner auf.
- **Mitglieder** – Listet alle Benutzer auf, die den einzelnen Benutzergruppen der verwalteten Rechner angehören.

Systeminformationen

Audit > Individuelle Daten anzeigen > Systeminformationen

- Ähnliche Informationen werden auch unter "Infocenter > Berichterstellung > Berichte > Inventarisierung *(siehe 206)*" angezeigt.

Auf der Seite **Systeminformationen** werden alle DMI/SMBIOS-Daten angezeigt, die durch das Systeminformations-**Audit** *(siehe 615)* für eine ausgewählte Rechner-ID erfasst wurden.

Aktionen

Es kann vorkommen, dass Sie benutzerdefinierte Feldwerte oder auch die bei einem Systemaudit erfassten Daten eines Rechners bearbeiten möchten. Bearbeitungen der Auditdaten werden von nachfolgenden Systemaudits überschrieben, es sei denn, Sie entfernen die betreffenden Systemauditfelder aus der automatischen Erfassung. Bearbeitete Systemauditfelder und benutzerdefinierte Felder können auf der Seite "Agent > **Agent-Status** *(siehe 32)*" auf der Seite **Zusammengeführte Tabelle filtern** *(siehe 30)* und im Bericht **Gesamttabelle** *(siehe 206)* ausgewählt werden. Sie können die Änderungen der Werte von Datenelementen auch automatisieren, indem Sie den Befehl **updateSystemInfo()** *(siehe 117)* in einem Agent-Verfahren ausführen.

- **Rechnerdaten bearbeiten** – Bearbeitet die bei einem Systemaudit erfassten Daten eines Rechners. Die Werte in benutzerdefinierten Feldern können ebenfalls geändert werden.
- **Automatische Sammlung bearbeiten** – Heben Sie die Markierung einzelner Elemente auf, um sie vor Überschreibung durch nachfolgende Systemaudits zu schützen. Diese Optionen werden zusammen mit dem Dialogfeld **Rechnerdaten bearbeiten** verwendet.
- **Massenbearbeitung, benutzerdefiniert** – Ändert die Werte in benutzerdefinierten Feldern auf mehreren Rechnern.
  1. Wählen Sie mehrere Rechnerzeilen aus.
  2. Klicken Sie auf **Massenbearbeitung, benutzerdefiniert**.
  3. Wählen Sie in der Dropdown-Liste **Benutzerdefiniertes änderbares Feld** ein benutzerdefiniertes Feld aus.
  4. Ersetzen Sie den vorhandenen Wert, indem Sie:
     - ✓ Einen vorhandenen Ersatzwert aus der Dropdown-Liste auswählen ODER
     - ✓ Den Ersatzwert manuell eingeben.

Sie können eine unbegrenzte Anzahl von benutzerdefinierten Feldern mit Informationen über verwaltete Rechner pflegen. Benutzerdefinierte Felder können auch auf der Seite "Audit > **Rechnerübersicht** *(siehe 151)*" gepflegt werden. Benutzerdefinierte Felder werden in Ansichten, Verfahren und Berichten unterstützt. Benutzerdefinierte Berichte können jedoch höchstens 40 benutzerdefinierte Felder aufnehmen.

- **Neues benutzerdefiniertes Feld** – Erstellt ein neues benutzerdefiniertes Feld.

- **Benutzerdefiniertes Feld umbenennen** – Benennt ein benutzerdefiniertes Feld um.
- **Benutzerdefiniertes Feld löschen** – Löscht ein benutzerdefiniertes Feld.

Einen Rechner auswählen

Wählen Sie im mittleren Feld einen Rechner aus, um Informationen darüber anzuzeigen. Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen und , um die vorherige und nächste Seite anzuzeigen. In der Dropdown-Liste wird der erste Datensatz jeder Seite mit Daten in der *Sortierreihenfolge der ausgewählten Spalte auf dieser Seite* angezeigt.

Angezeigte Daten

- Systeminformationen
  - **Hersteller** – Systemhersteller
  - **Produktname** – Produktname des Systems
  - **Systemversion** – Versionsnummer des Produkts
  - **System-Seriennummer** – Seriennummer des Systems
- Netzwerkinformationen
  - **IPv4-Adresse** – Dem Rechner zugewiesene Version-4-IP-Adresse
  - **IPv6-Adresse** – Dem Rechner zugewiesene Version-6-IP-Adresse
  - **Subnetz-Maske** – Dem Rechner zugewiesenes Netzwerksubnetz.
  - **Standard-Gateway** – Dem Rechner zugewiesener Standard-Gateway.
  - **Verbindungs-Gateway** – Die vom Kaseya Server erkannte IP-Adresse, wenn dieser Rechner eingecheckt wird. Befindet sich der Rechner hinter einem DHCP-Server, ist dies die öffentliche IP-Adresse des Subnetzes.
  - **Land** – Mit dem Connection-Gateway verknüpftes Land.
  - **MAC-Adresse** – MAC-Adresse der LAN-Karte, die zur Kommunikation mit dem Kaseya Server verwendet wird
  - **DHCP-Server** – IP-Adresse des von diesem Rechner verwendeten DHCP-Servers.
  - **DNS-Server 1, 2** – IP-Adresse des dem Rechner zugewiesenen DNS-Servers.
- Gehäuse
  - **Gehäusehersteller** – Hersteller des Gehäuses
  - **Gehäusetyp** – Typ des Gehäuses
  - **Gehäuseversion** – Versionsnummer des Gehäuses
  - **Max. Speichersteckplätze** – Gesamtzahl der verfügbaren Speichermodulsteckplätze
  - **Gehäuse-Seriennummer** – Seriennummer auf dem Gehäuse
  - **Gehäuse-Bestandsetikett** – Bestandsetikett auf dem Gehäuse
- Hauptplatine
  - **Hauptplatinenhersteller** – Hersteller der Hauptplatine
  - **Hauptplatinenprodukt** – Produkt-ID der Hauptplatine
  - **Hauptplatinenversion** – Versionsnummer der Hauptplatine
  - **Hauptplatinen-Seriennummer** – Seriennummer der Hauptplatine
  - **Externe Busgeschwindigkeit** – Busgeschwindigkeit der Hauptplatine
- CPU/RAM-Daten
  - **Prozessorhersteller** – Hersteller des Prozessors
  - **Prozessorfamilie** – Installierter Prozessortyp
  - **Prozessorversion** – Versions-ID des Prozessors
  - **Max. CPU-Geschwindigkeit** – Maximal unterstützte Prozessorgeschwindigkeit

- **Aktuelle CPU-Geschwindigkeit** – Aktuelle Geschwindigkeit, mit der der Prozessor ausgeführt wird
- **Prozessor** – Prozessorversion und -modell
- **Menge** – Anzahl der Prozessoren
- **Geschwindigkeit** – Taktgeschwindigkeit des Prozessors.
- **RAM**– Größe des Arbeitsspeichers des Rechners in MB
- **Max. Speichergröße** – Maximale Speichergröße der Hauptplatine
- **Max. Speichersteckplätze** – Gesamtzahl der verfügbaren Speichermodulsteckplätze.

- **Benutzerdefinierte Felder** – Benutzerdefinierte Felder und deren Werte
- **Integrierte Geräte** – Liste der auf der Hauptplatine basierten Geräte (wie Video oder Ethernet)
- **Portverbinder** – Liste der auf dem Gehäuse verfügbaren Anschlüsse
- **Speichergeräte** – Liste der auf der Hauptplatine installierten Speichermodule
- **Systemsteckplätze** – Status aller verfügbaren Kartensteckplätze

Installierte Anwendungen

Audit > Individuelle Daten anzeigen > Installierte Anwendungen

- Ähnliche Informationen werden auch unter "Infocenter > Berichterstellung > Berichte > Software - Software-Anwendungen installiert *(siehe 235)*" angezeigt.

Auf der Seite "Installierte Anwendungen" werden alle Anwendungen aufgelistet, die während des **letzten Audits** *(siehe 615)* für eine ausgewählte Rechner-ID gefunden wurden. Die Liste der auswählbaren Rechner-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem verwendeten **Scope** *(siehe 419)*. Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(siehe 18)*.

Einen Rechner auswählen

Wählen Sie im mittleren Feld einen Rechner aus, um Informationen darüber anzuzeigen. Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen und , um die vorherige und nächste Seite anzuzeigen. In der Dropdown-Liste wird der erste Datensatz jeder Seite mit Daten in der *Sortierreihenfolge der ausgewählten Spalte auf dieser Seite* angezeigt.

Die folgenden Informationen werden angezeigt:

- **Anwendung** – Der Dateiname der Anwendung.
- **Beschreibung** – Eine kurze Beschreibung der Anwendung laut Angabe im Dialogfeld 'Eigenschaften' der ausführbaren Datei.
- **Version** – Die Versionsnummer der Anwendung.
- **Hersteller** – Der Hersteller der Anwendung.
- **Produktname** – Der Produktname der Anwendung
- **Verzeichnispfad** – Der vollständige Verzeichnispfad der Anwendung.
- **Dateigröße** – Die Größe der Anwendungsdatei in Kilobyte.
- **Letzte Änderung** – Das letzte Änderungsdatum der Anwendungsdatei.

Hinweis: Mit den Optionen **Enthält/Fehlende Anwendung** und **Versionszeichenfolge ist > < = N** in **Ansichtsdefinitionen** *(siehe 27)* können Sie die Anzeige der Rechner-IDs auf jeder Agent-Seite filtern.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen und , um die vorherige und nächste Seite anzuzeigen. In der

Dropdown-Liste wird der erste Datensatz jeder Seite mit Daten in der *Sortierreihenfolge der ausgewählten Spalte auf dieser Seite* angezeigt.

Hinzufügen/Entfernen

Audit > Individuelle Daten anzeigen > Hinzufügen/Entfernen

- Ähnliche Informationen werden auch unter "Infocenter > Berichterstellung > Berichte > Software" angezeigt.
- Alarme können unter "Monitoring > Alarme > Anwendungsänderungen *(siehe 289)*" definiert werden.

Auf der Seite **Hinzufügen/Entfernen** werden die Programme angezeigt, die im Fenster **Programme hinzufügen/entfernen** des verwalteten Rechners aufgelistet werden. Die auf dieser Seite gezeigten Informationen werden beim Durchführen einer **letzten Inventarisierung** *(siehe 146)* erfasst. Klicken Sie auf eine Rechner-ID, um die Daten für den ausgewählten Rechner anzuzeigen. Die Liste der auswählbaren Rechner-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem verwendeten **Scope** *(siehe 419)*.

Einen Rechner auswählen

Wählen Sie im mittleren Feld einen Rechner aus, um Informationen darüber anzuzeigen. Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen und , um die vorherige und nächste Seite anzuzeigen. In der Dropdown-Liste wird der erste Datensatz jeder Seite mit Daten in der *Sortierreihenfolge der ausgewählten Spalte auf dieser Seite* angezeigt.

Die folgenden Informationen werden angezeigt:

- **Anwendungsname** – Der Name der Anwendung
- **Zeichenfolge deinstallieren** – Die Deinstallationszeichenfolge in der Registrierung, mit der die Anwendung deinstalliert wird

Softwarelizenzen

Audit > Individuelle Daten anzeigen > Softwarelizenzen

- Ähnliche Informationen werden auch unter "Infocenter > Berichterstellung > Berichte > Software" angezeigt.

Auf der Seite **Softwarelizenzen** werden alle Softwarelizenzen angezeigt, die für die ausgewählte Rechner-ID gefunden wurden.Die Liste der angezeigten Rechner-IDs ist abhängig vom **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, zu deren Anzeige der Benutzer über System > Benutzersicherheit > **Scopes** *(siehe 419)* autorisiert ist.

Die auf dieser Seite gezeigten Informationen werden beim Durchführen einer **letzten Inventarisierung** *(siehe 146)* erfasst. Jeder Hersteller speichert den Lizenzschlüssel seiner Anwendung anders. Daher ist es möglich, dass nicht alle Softwarelizenzen von Anwendungen erfasst werden.

Doppelte Lizenzschlüssel

Doppelte Lizenzschlüsse, die auf mehr als einem Rechner gefunden werden, werden als roter Text angezeigt. Durch Klicken auf den Nummern-Link neben dem Titel einer doppelten Lizenz werden die Rechner-IDs aufgelistet, die die doppelte Lizenz verwenden.

Einen Rechner auswählen

Wählen Sie im mittleren Feld einen Rechner aus, um Informationen darüber anzuzeigen. Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen und , um die vorherige und nächste Seite anzuzeigen. In der Dropdown-Liste wird der erste Datensatz jeder Seite mit Daten in der *Sortierreihenfolge der ausgewählten Spalte auf dieser Seite* angezeigt.

Die folgenden Informationen werden angezeigt:

- **Herausgeber** – Der Herausgeber der Softwareanwendung (z. B. Microsoft)
- **Titel** – Der Name der Anwendung
- **Produktschlüssel** – Der bei der Installation zum Aktivieren der Anwendung verwendete Produktschlüssel
- **Lizenz** – Der mit der Anwendung verknüpfte Lizenzschlüssel
- **Version** – Die Version der Anwendung
- **Datum** – Das Freigabedatum dieser Version

Dokumente

Audit > Individuelle Daten anzeigen > Dokumente

- Auf diese Funktion kann auch über die Registerkarte "Dokumente" der Seite Live-Connect *(siehe 393)* > Agent-Daten" bzw. der Seite Rechnerübersicht *(siehe 151)* zugegriffen werden.

Auf der Seite **Dokumente** werden alle Dateien angezeigt, die mit einer Rechner-ID verknüpft sind. Sie können beispielsweise gescannte Kopien von Kaufbelegen, Vertragsinformationen und Konfigurationsanmerkungen für eine bestimmte Rechner-ID hochladen. Die hochgeladenen Dokumente werden im Verzeichnis der Benutzerprofile des Kaseya Server abgelegt. Zum Beispiel: `C:\Kaseya\UserProfiles\368905064566500\Docs`.

Hinweis: Dokumente werden bei der Sicherung der Kaseya Server-Datenbank mit "System > **Konfigurieren** *(siehe 429)*" nicht berücksichtigt. Es sollte daher eine separate Sicherung der Kaseya Server-Dateien und -Verzeichnisse durchgeführt werden.

Hinweis: Unter **Administratorhinweise** *(siehe 14)* finden Sie eine schnelle Möglichkeit zur Protokollierung von Nur-Text-Anmerkungen für mehrere Rechner, ohne Dokumente hochzuladen zu müssen.

So speichern Sie ein Dokument:

1. Klicken Sie auf einen Rechner.Gruppen-ID-Link. Die Liste der auswählbaren Rechner-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem verwendeten **Scope** *(siehe 419)*. Dokumente, die zuvor auf dem Kaseya Server für diese Rechner-ID gespeichert waren, werden angezeigt. Andernfalls erhalten Sie die Meldung `No files found`.
2. Klicken Sie auf **Durchsuchen**, um eine Datei auf dem lokalen Computer oder im LAN zu ermitteln.
3. Klicken Sie auf **Hochladen**, um die Datei auf den Kaseya Server hochzuladen.

   Der hinzugefügte **Dateiname** wird zusammen mit der **Dateigröße** und dem Datum und der Uhrzeit des **letzten Upload** angezeigt.

Neuer Ordner

Klicken Sie wahlweise auf das Symbol und den Link für **Neuer Ordner**, um einen neuen Ordner zu erstellen, in dem Dokumente für den ausgewählten verwalteten Rechner gespeichert werden.

Bearbeiten

Sie können auf einen **Dateiname**-Link oder das Bearbeitungssymbol klicken, um eine Datei anzuzeigen oder auszuführen. Dies hängt von der Anwendung ab, mit der die Dateinamenerweiterung auf Ihrem lokalen Rechner verknüpft ist.

Löschen

Klicken Sie auf das Löschen-Symbol , um ein gespeichertes Dokument oder einen Ordner auf dem Kaseya Server zu löschen.

Kapitel 6

Infocenter

In diesem Kapitel

Posteingang

Info Center > Desktop > Posteingang

Im **Posteingang** werden alle eingehenden Nachrichten angezeigt, die Ihnen von anderen VSA-Benutzern oder aufgrund von Systemereignissen gesendet wurden. Systemereignisse umfassen Folgendes:

- **Reporting** – Über die Seiten **Berichte**, **Berichtssets** und **Planung** kann bei der Berichtserstellung eine Posteingangsnachricht generiert werden, sofern ein Benutzer als Nachrichtenempfänger angegeben wurde.
- **Service Desk** – Bei **Service Desk**-Verfahren kann das Senden einer Nachricht an einen oder mehrere Benutzer ausgelöst werden. Durch **Service Desk** generierte Nachrichten werden über Service Desk > Nachrichtenvorlagen formatiert.

Hinweis: Nachrichten im **Posteingang** werden nicht archiviert.

Aktionen

- **Neu** – Erstellt eine neue Nachricht an einen anderen VSA-Benutzer.
- **Weiterleiten** – Leitet eine ausgewählte Nachricht an einen anderen VSA-Benutzer weiter.
- **Antworten** – Beantwortet eine ausgewählte Nachricht von einem anderen VSA-Benutzer.
- **Löschen** – Löscht ausgewählte Nachrichten.
- **Lesen** –Markiert ausgewählte Nachrichten als gelesen.
- **Nicht gelesen** – Markiert ausgewählte Nachrichten als nicht gelesen.
- **Aktualisieren** – Aktualisiert die Seite.

Bearbeitung

Bei **Neu**, **Weiterleiten** und **Antworten**:

- Klicken Sie auf die Symbole To Cc, um einen oder mehrere VSA-Benutzer auszuwählen, an die eine Nachricht gesendet werden soll. Sie können die Liste der Benutzer, aus der eine Auswahl getroffen werden soll, filtern.
- Über die folgenden Schaltflächen in der Werkzeugleiste können Sie eine besondere Formatierung zum Text hinzufügen:



  - – Hyperlink für ausgewählten Text. Möglicherweise müssen Sie Links, die von einer anderen Quelle eingefügt wurden, zurücksetzen.
  - – Tabelle einfügen
  - – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
  - – Text einrücken
  - – Text ausrücken
  - – Formatierung entfernen
  - Ω – Symbol einfügen
  - – Emoticon einfügen
  - – Vorschau der Darstellung von Text und Bildern anzeigen
  - – Datei oder Bild hochladen
  - x_2 – Ausgewählten Text tiefgestellt festlegen

- x² – Ausgewählten Text hochgestellt festlegen
- – Vollbildmodus für die Bearbeitung und die Anzeige ein- und ausschalten

Planung

Info Center > Reporting > Planung

Auf der Berichtseite **Planung** sind alle Berichte und Berichtssets aufgeführt, die *unter demselben Scope, den Sie aktuell verwenden, veröffentlicht wurden.* Falls Ihre Nachrichten und E-Mails unter Info Center > **Posteingang** *(siehe 162)* gelöscht wurden, können Sie weiterhin einen veröffentlichten Bericht lokalisieren, für den Sie **Anzeigerechte** *(siehe 171)* besitzen.

Klicken Sie auf das Symbol neben dem Namen des Berichts oder des Berichtssets , um das Dialogfeld **Verlauf ausgewählter Elemente** mit dem Veröffentlichungsverlauf dieses Berichts anzuzeigen. Klicken Sie auf das Veröffentlichungsdatum des Berichts, den Sie anzeigen möchten, und klicken Sie dann unten im Dialogfeld auf den Hyperlink dieses Berichts. Verwenden Sie das gleiche Dialogfeld zum **Genehmigen/Ablehnen** *(siehe 171)* eines Berichts.

Aktionen

- **Jetzt ausführen** – Führt einen bereits geplanten Bericht oder ein geplantes Berichtsset unverzüglich aus. Hiermit können Sie Berichte, für die eine Zeitüberschreitung aufgetreten ist, ein Fehler generiert wurde oder keine Genehmigung vorliegt, sofort erneut ausführen, ohne dass sämtliche Planungsoptionen nochmals gewählt werden müssen.
- **Empfänger** – Zeigt die Registerkarte **Verteilung** des Dialogfelds **Ausgewähltes Element neu planen** *(siehe 168)* an. Ändern Sie auf dieser Registerkarte die Empfänger für einen ausgewählten Bericht, den Sie erneut planen. *Diese Optionen sind mit denen bei der ursprünglichen Planung eines Berichts identisch.*
- **Verlauf** – Hierdurch wird das Dialogfeld **Verlauf ausgewählter Elemente** aufgerufen, in dem alle veröffentlichten Instanzen eines empfangenen Berichts oder Berichtssets aufgeführt sind. Klicken Sie auf das Veröffentlichungsdatum der Berichte oder Berichtssets, die Sie anzeigen möchten, und klicken Sie dann unten im Dialogfeld auf den entsprechenden Hyperlink. Verwenden Sie das gleiche Dialogfeld zum **Genehmigen/Ablehnen** *(siehe 171)* eines Berichts.
- **Planung läuft**
  - **Neu** – Plant beliebige Berichte, zu deren Veröffentlichung Sie berechtigt sind.
  - **Bearbeiten** – Zeigt die Registerkarte **Planung** des Dialogfelds **Ausgewähltes Element neu planen** *(siehe 168)* an. Planen Sie auf dieser Registerkarte die Veröffentlichung eines ausgewählten Berichts oder Berichtssets neu. *Diese Optionen sind mit denen bei der ursprünglichen Planung eines Berichts identisch.*
  - **Löschen** – Löscht einen ausgewählten veröffentlichten Bericht oder ein Berichtsset endgültig. Hierdurch wird nur der Datensatz des Berichts unter **Planung** für Ihre VSA-Anmeldung gelöscht. Der Bericht wird jedoch *nicht* für andere Benutzer gelöscht.
- **Aktualisieren** – Aktualisiert die Seite.

Tabellenspalten

Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(siehe 18)*.

- **(Status)**
  - Anstehend
  - Abgeschlossen und Genehmigung erforderlich – Klicken Sie auf das Symbol , um den abgeschlossenen Bericht anzuzeigen und ihn dann zu genehmigen oder abzulehnen. Siehe **Genehmigen/Ablehnen von Berichten** *(siehe 171)*.

- ➢ Abgeschlossen und abgelehnt – Klicken Sie auf das Symbol um den abgeschlossenen und abgelehnten Bericht anzuzeigen. Sie können ihn im Nachhinein noch genehmigen.
- ➢ Abgeschlossen und verteilt – Klicken Sie auf das Symbol neben dem Namen des Berichts, um das Dialogfeld **Verlauf ausgewählter Elemente** mit dem Veröffentlichungsverlauf dieses Berichts anzuzeigen. Klicken Sie auf das Veröffentlichungsdatum des Berichts, den Sie anzeigen möchten, und klicken Sie dann unten im Dialogfeld auf den Hyperlink dieses Berichts.
- ➢ Fehler – Der Bericht konnte nicht veröffentlicht werden.

- **Name** – Der Name des Berichts.
- **Eigentümer** – Der Ersteller des Berichts.
- **Wiederholung** – Klicken Sie auf die Wiederholung – `Einmal`, `Täglich`, `Wöchentlich`, `Monatlich` – um die Planung entsprechend zu aktualisieren.
- **Empfänger** – Klicken Sie auf die Anzahl von Empfängern, um die Liste der Empfänger im Dialogfeld **Ausgewähltes Element neu planen** *(siehe 168)* zu aktualisieren.
- **Empfängerliste** – Eine Liste von Empfängern
- **Zuletzt ausgeführt** – Die Zeit der letzten Veröffentlichung des Berichts
- **Nächster Durchlauf** – Die Zeit der nächsten geplanten Veröffentlichung des Berichts
- **Organisation, Rechnergruppe, Rechner, Ansicht** – Die **Datenfilter** *(siehe 168)*-Typen, mit denen die Daten in einem Bericht eingegrenzt werden. Verwenden Sie eine Ansicht, um mehr als eine Organisation, Rechnergruppe oder einen Rechner auszuwählen. Alle Rechnergruppen in allen Organisationen, die Sie gemäß Ihrem Scope anzeigen dürfen, sind standardmäßig ausgewählt.
- **Typ** – `Bericht` oder `Berichtsset`
- **Status** – Der Status des Berichts in Textformat
- **Ort** – Der Ordner, in dem der geplante Bericht sich befindet (mittlerer Fensterbereich)
- **Erstellungsdatum** – Das Datum, an dem der Bericht geplant war.
- **Scope** – Die Sichtbarkeit der Zeilen in der Tabelle 'Planung' wird durch den verwendeten Scope eingeschränkt. Ihr Scope muss mit dem Scope übereinstimmen, der bei der Planung des Berichts durch den Eigentümer aktuell war. Hierdurch wird sichergestellt, dass nur Benutzer, die zur Einsicht der gleichen im Bericht angezeigten Daten berechtigt sind, die Empfänger des Berichts neu planen und ändern können. E-Mail-Empfänger haben per E-Mail auf den abgeschlossenen Bericht immer Zugriff, selbst, wenn sie nicht Mitglieder des gleichen Scopes sind.

Berichte

Info Center > Reporting > Berichte

Virtual System Administrator™ bietet umfassende Berichterstellung für alle Anwendungen. **Berichte** *(siehe 164)* können mithilfe von Berichtsparametern angepasst und nach Organisation, Rechnergruppe, Rechner-ID oder Ansichtsdefinition gefiltert werden. Sie können Berichte im PDF-, HTML- oder Excel-Format ausgeben und diese mit Ihrem eigenen Logo, Deckblatt sowie einer Kopf- und Fußzeile kennzeichnen. Berichte können automatisch ausgeführt und regelmäßig geplant werden. Sie können privat oder gemeinsam genutzt sowie an den **Posteingang** *(siehe 162)* von VSA-Benutzern oder an E-Mail-Empfänger weitergeleitet werden. Ein optionaler Schritt "Bestätigung erforderlich" wird unmittelbar vor der Verteilung bereitgestellt. Berichte können auch zu **Berichtssätzen gebündelt werden** *(siehe 172)*, sodass Sie in der Lage sind, eine Standardgruppe von Berichten zu planen. In der Liste Ihrer eigenen **geplanten** *(siehe 163)* Berichte wird jeder Bericht aufgeführt, auf den Sie zugreifen können. Sie können also jederzeit anstehende Berichte, die Sie erstellt und geplant haben, oder beliebige Berichte, die Sie erhalten haben, ermitteln.

Einen Überblick über das Arbeiten mit Berichten erhalten Sie unter den folgenden Themen:

- **Berichtsdefinitionen** *(siehe 165)*

- **Berichtsordnerstrukturen** *(siehe 166)*
- **Sofortiges Veröffentlichen von Berichten** *(siehe 167)*
- **Datenfilter** *(siehe 168)*
- **Planung/erneute Planung von Berichten** *(siehe 168)*
- **Verwalten von geplanten Elementen** *(siehe 169)*
- **Genehmigen/Ablehnen von Berichten** *(siehe 171)*
- **Benutzersicherheit bei Berichten und Berichtssets** *(siehe 171)*
- **Alte Berichtsdefinitionen** *(siehe 203)*

Begriffe und Konzepte

- **Veröffentlichte Berichte** – Veröffentlichte Berichte enthalten das Layout und die Daten für ein bestimmtes Datum, die Uhrzeit, den Scope und andere Kriterien und werden an eine ausgewählte Gruppe von Empfängern verteilt. Um im selben Bericht neue Daten zu sehen, muss der Bericht neu veröffentlicht und neu verteilt werden.
- **Berichtsdefinitionen** – Ein Bericht wird basierend auf einer Berichtsdefinition veröffentlicht. Berichtsdefinitionen enthalten alle *Standard*einstellungen, mit denen Inhalt, Layout und Dateiformat eines veröffentlichten Berichts festgelegt werden. Sie können beim Veröffentlichen des Berichts diese Standardeinstellungen überschreiben.
- **Berichtsvorlagen** – Zur Erstellung einer Berichtsdefinition werden Einstellungen aus einer Berichtsvorlage kopiert. Berichtsvorlagen definieren alle *Standard*-Einstellungen für eine Berichtsdefinition. Es gibt zwei Arten von Berichtsvorlagen:
  - **Benutzerdefiniert** – Anpassbare Berichtsvorlagen
  - **Legacy** – **In früheren Versionen bereitgestellte Berichtsvorlagen mit einem festgelegten Layout** *(siehe 203)*
- **Berichtskategorien** – Berichtsvorlagen werden nach Berichtsvorlagenkategorien organisiert.

Berichtsdefinitionen

Ein Bericht wird basierend auf einer Berichtsdefinition veröffentlicht. Berichtsdefinitionen enthalten alle *Standard*einstellungen, mit denen Inhalt, Layout und Dateiformat eines veröffentlichten Berichts festgelegt werden. Sie können beim Ausführen (Veröffentlichen) oder Planen des Berichts diese Standardeinstellungen überschreiben.

Beim Erstellen einer Berichtsdefinition werden Berichtsdefinitionseinstellungen aus einer Berichtsvorlage kopiert. Durch das Ändern einer Berichtsdefinition wird nicht die Berichtsvorlage, aus der sie kopiert wurde, geändert. An einer Berichtsvorlage vorgenommene Änderungen haben keine Auswirkungen auf die Berichtsdefinitionen, die bereits aus dieser Vorlage kopiert wurden.

So erstellen Sie eine *benutzerdefinierte Berichtsdefinition* basierend auf einer *Berichtsvorlage*:

1. Klicken Sie auf **Info Center > Reporting > Berichte > Neu**.
2. Wählen Sie die benutzerdefinierte Option **Bericht**.
3. Wählen Sie eine **Kategorie**, dann eine **Vorlage** und klicken Sie anschließend auf **Erstellen**.

> **Hinweis:** Eine benutzerdefinierte Berichtsvorlage muss **veröffentlicht** *(siehe 174)* sein, damit Sie sie in der Kategorie **Berichte** *(siehe 164)* sehen können.

4. Geben Sie unter Verwendung der Kopfzeilenoptionen und dreier Registerkarten Optionen für Berichtsdefinitionen an:
   - **(Kopfzeilenoptionen)** – Geben Sie den Namen und Titel des Berichts an. Außerdem können Sie festlegen, dass **für den Bericht eine Genehmigung erforderlich** *(siehe 171)* ist.
   - **Layout** – Eine Beschreibung dieser Optionen finden Sie unter **Berichtsvorlagen** *(siehe 174)*.

> **Hinweis:** Beim Hinzufügen oder Bearbeiten einer **alten Berichtsdefinition** *(siehe 203)* wird die Registerkarte **Parameter** statt der Registerkarte **Layout** angezeigt.

- **Allgemein** – Bestimmt die Art der Ausgabe – PDF, HTML oder EXCEL –, Papiergröße und Ausrichtung. Mit dieser Option wird außerdem die Nachricht festgelegt, mit der Benutzer über den Zeitpunkt der Ausführung des Berichts benachrichtigt werden. Tokens können in E-Mail-Nachrichten für Berichte – sowohl in der Betreffzeile als auch im Nachrichtentext – mit aufgenommen werden.
  - ✓ `<gr>` – Rechnergruppe
  - ✓ `<id>` – Rechner-ID
  - ✓ `<rt>` – Berichtsname
  - ✓ `<embd>` – Sie können nur im Nachrichtentext einen HTML-Bericht an der angegebenen Stelle einbetten.

  Über die Werkzeugleiste zum Bearbeiten können Sie Bilder und eine besondere Formatierung zum Text hinzufügen. Bilder müssen hochgeladen anstatt kopiert und eingefügt werden.

  - ✓ – Hyperlink für ausgewählten Text. Möglicherweise müssen Sie Links, die von einer anderen Quelle eingefügt wurden, zurücksetzen.
  - ✓ – Tabelle einfügen
  - ✓ – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
  - ✓ – Text einrücken
  - ✓ – Text ausrücken
  - ✓ – Formatierung entfernen
  - ✓ Ω – Symbol einfügen
  - ✓ – Emoticon einfügen
  - ✓ – Bild- und Textvorschau anzeigen
  - ✓ – Datei oder Bild hochladen
  - ✓ x_2 – Ausgewählten Text tiefgestellt festlegen
  - ✓ x^2 – Ausgewählten Text hochgestellt festlegen
  - ✓ – Vollbildmodus zur Ansicht und Bearbeitung ein- und ausschalten
- **Deckblatt, Kopf- und Fußzeile** – Hierdurch werden **Deckblatt, Kopf- und Fußzeile** *(siehe 201)* des Berichts ausgewählt

Berichtsordnerstrukturen

Berichtsdefinitionen werden mithilfe von zwei Ordnerstrukturen im mittleren Feld unterhalb der Cabinets **Privat** und **Gemeinsam nutzen** organisiert. Verwenden Sie die folgenden Optionen, um Objekte in diesen Ordnerstrukturen zu verwalten:

Immer verfügbar

- **(Filter anwenden)** – Geben Sie Text in das Bearbeitungsfeld des Filters ein und klicken Sie dann auf das Trichtersymbol, um das Filtern auf die Ordnerstrukturen anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in den Ordnerstrukturen gefunden wird.

Bei Auswahl eines Cabinets

- **Alle ausblenden** – Blendet alle Verzweigungen der Ordnerstruktur aus.
- **Alle erweitern** – Zeigt alle Verzweigungen der Ordnerstruktur an.

Bei Auswahl eines Ordners

- **Ordnereigenschaften** – Ordnereigenschaften werden im rechten Bereich angezeigt und führen den Eigentümer und die gültigen **Rechte** *(siehe 125)* für den Ordner auf.
- **Neu**
  - **Ordner** – Erstellt einen neuen Ordner unterhalb des ausgewählten Cabinets oder Ordners.
  - **Bericht** – Erstellt im ausgewählten Ordner der Ordnerstruktur eine *benutzerdefinierte* **Berichtsdefinition**.
  - **Alte165r Bericht** – Erstellt im ausgewählten Ordner der Ordnerstruktur eine **alte Berichtsdefinition** *(siehe 203)* .
- **Löschen** – Löscht einen ausgewählten Ordner.
- **Umbenennen** – Benennt einen ausgewählten Ordner um.
- **Gemeinsam nutzen** – Dies gilt nur für **gemeinsam genutzte** genutzte Cabinet-Ordner. Hierdurch wird ein Ordner mit Benutzerrollen und einzelnen Benutzern freigegeben. Richtlinien zu den Freigaberechten für Objekte in Ordnerstrukturen finden Sie unter dem Thema **Ordnerrechte** *(siehe 125)*.

Bei Auswahl einer Berichtsdefinition

- **Neu**
  - **Bericht** – Erstellt im ausgewählten Ordner der Ordnerstruktur eine *benutzerdefinierte* **Berichtsdefinition**.
  - **Alte165r Bericht** – Erstellt im ausgewählten Ordner der Ordnerstruktur eine **alte Berichtsdefinition** *(siehe 203)* .
- **Bearbeiten** – Bearbeitet die ausgewählte Berichtsdefinition.
- **Kopieren** – Kopiert die ausgewählte Berichtsdefinition.
- **Als Vorlage festlegen** – Dies gilt nur für benutzerdefinierte **Berichtsdefinitionen** *(siehe 165)*. Hierdurch wird eine Berichtsdefinition in einem ausgewählten **Berichtsvorlagen** *(siehe 174)*-Ordner gespeichert. Beispielsweise können Benutzer nützliche Verbesserungen für ihre eigenen Berichtsdefinitionen erstellen. Diese wiederum lassen sich in Berichtsvorlagen umwandeln, auf die andere Benutzer ihre eigenen Berichtsdefinitionen basieren können.
- **Löschen** – Löscht die ausgewählte Berichtsdefinition.
- **Jetzt ausführen** – Basierend auf der ausgewählten Berichtsdefinition wird **ein Bericht sofort ausgeführt** *(siehe 167)*.
- **Planung** – Basierend auf der ausgewählten Berichtsdefinition wird **die Veröffentlichung eines Berichts geplant** *(siehe 168)*.

> **Hinweis:** Die Schaltfläche **Planung** ist möglicherweise für Standardbenutzer ausgeblendet. Diese Schaltfläche wird über den Knoten System > Systemvoreinstellungen > Planung aktivieren auf der Registerkarte **Benutzerrollen – Zugriffsrechte** *(siehe 415)* aktiviert.

Sofortiges Veröffentlichen von Berichten

Wählen Sie unter einer der **Berichtsordnerstrukturen** *(siehe 166)* einen Bericht und klicken Sie dann auf **Jetzt ausführen**, um das Dialogfeld **Datenfilter** *(siehe 168)* anzuzeigen. Mit **Jetzt ausführen** veröffentlichte Berichte werden *nicht* der Liste der geplanten veröffentlichten Berichte hinzugefügt und werden nur dem aktuellen Benutzer angezeigt.

Datenfilter

Datenfilter grenzen die in einem Bericht enthaltenen Daten ein. Sie werden jedes Mal angezeigt, wenn die Schaltfläche **Jetzt ausführen** geklickt wird, oder als Registerkarte, wenn die Schaltfläche **Planung** geklickt wird.

- **Organisation, Rechnergruppe**, **Rechner-ID** und **Ansicht wählen**
  - Filtern Sie die Auswahl der in den Bericht eingeschlossenen Daten nach Organisation, Rechnergruppe, Rechner-ID oder Ansicht.
  - Wenn keine Ansicht gewählt ist, werden alle Rechnergruppen in allen Organisationen, die Sie gemäß Ihrem Scope anzeigen dürfen, standardmäßig ausgewählt.
  - Die Datenfilterung **Jetzt ausführen** wird standardmäßig von dem Rechner-ID- bzw. dem Gruppen-ID-Filter übernommen.
  - Für manche Berichte ist eine Abteilungsfilter und ein Service Desk-Filter verfügbar.
- **Sprache** – Sie können die Sprache wählen, in der ein Bericht präsentiert werden soll. Die Sprachoption wird allerdings nur angezeigt, wenn Sprachpakete installiert sind. Siehe System > **Voreinstellungen** *(siehe 402)*.
- **Datumsfilter** – Bei *benutzerdefinierten* Berichtsdefinitionen werden die folgenden **Datumsfilter**optionen nur angezeigt – zumindest für einen Teil in der Konfiguration der Berichtsdefinition –, wenn `Übernehmen von Bericht` und eine *Datums-/Zeitspalte* für die Datumsfilterung ausgewählt wurden.
  - Vordefinierte Bereiche – `Diese Woche`, `Letzte Woche`, `Dieser Monat`, `Letzter Monat`, `Dieses Quartal`, `Letztes Quartal`.
  - `Letzte N Tage` – Geben Sie den Wert `N` im Feld **Anzahl der Tage** ein.
  - `Festgelegter Bereich` – Geben Sie **Startdatum/-zeit** und **Enddatum/-zeit** ein.

Planung/erneute Planung von Berichten

Wählen Sie unter einer der **Berichtsordnerstrukturen** *(siehe 166)* einen Bericht und klicken Sie dann auf **Planung**, um ein Dialogfeld mit vier Registerkarten anzuzeigen. Planen Sie in diesem Dialogfeld die Veröffentlichung des Berichts für die Zukunft, entweder einmalig oder zu regelmäßig wiederkehrenden Terminen. *Diese Einstellungen gelten nur für diese spezifische Planung des Berichts. Die Berichtsdefinition bleibt unverändert.* Durch Klicken der Schaltfläche **Abschicken** wird der Bericht mit den aktuell auf allen vier Registerkarten ausgewählten Einstellungen veröffentlicht.

Ein ähnliches Dialogfeld namens **Ausgewähltes Element neu planen** wird angezeigt, wenn Sie einen vormals geplanten Bericht **neu planen**.

- **Planung** – Planen Sie die einmalige oder die wiederholte Ausführung des Berichts. Jede Art der Wiederholung (einmal, täglich, wöchentlich, monatlich, jährlich) zeigt weitere Optionen für diese Art der Wiederholung an. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen.
- **Filter** – Siehe **Datenfilter** *(siehe 168)*
- **Verteilung** – Wählen Sie die Empfänger des Berichts aus.
  - Im oberen Bereich namens **Verteilung** wird standardmäßig die Person, die den Bericht ausführt oder plant, als ein Info Center > **Posteingang** *(siehe 162)*-Nachrichtenempfänger ausgewählt.
  - Sie können zusätzliche Benutzer aus dem unteren Bereich in den oberen **Verteilungs**bereich ziehen und dort ablegen. Für **Mitarbeiter** *(siehe 426)* muss eine E-Mail-Adresse im unteren Bereich angezeigt werden.
  - Die Benutzer, die Ihnen angezeigt werden, sind auf den gleichen Scope beschränkt, den Sie bei der Planung bzw. erneuten Planung des Berichts verwenden.
  - Jedem Benutzer im oberen **Verteilungs**bereich kann der gleiche Bericht als E-Mail-Empfänger zugeschickt werden.

- Sie können im Bearbeitungsfeld **Zusätzliche E-Mail** E-Mail-Adressen *für Benutzer außerhalb des von Ihnen verwendeten Scopes* hinzufügen. Geben Sie die E-Mail-Adressen manuell, durch Semikolons getrennt, ein.

- **Allgemein** – Bestimmt die Art der Ausgabe – PDF, HTML oder EXCEL –, Papiergröße und Ausrichtung. Mit dieser Option wird außerdem die Nachricht festgelegt, mit der Benutzer über den Zeitpunkt der Ausführung des Berichts benachrichtigt werden. Tokens können in E-Mail-Nachrichten für Berichte – sowohl in der Betreffzeile als auch im Nachrichtentext – mit aufgenommen werden.
  - `<gr>` – Rechnergruppe
  - `<id>` – Rechner-ID
  - `<rt>` – Berichtsname
  - `<embd>` – Sie können nur im Nachrichtentext einen HTML-Bericht an der angegebenen Stelle einbetten.

  Über die Werkzeugleiste zum Bearbeiten können Sie Bilder und eine besondere Formatierung zum Text hinzufügen. Bilder müssen hochgeladen anstatt kopiert und eingefügt werden.



  - – Hyperlink für ausgewählten Text. Möglicherweise müssen Sie Links, die von einer anderen Quelle eingefügt wurden, zurücksetzen.
  - – Tabelle einfügen
  - – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
  - – Text einrücken
  - – Text ausrücken
  - – Formatierung entfernen
  - – Symbol einfügen
  - – Emoticon einfügen
  - – Vorschau der Darstellung von Text und Bildern anzeigen
  - – Datei oder Bild hochladen
  - – Ausgewählten Text tiefgestellt festlegen
  - – Ausgewählten Text hochgestellt festlegen
  - – Vollbildmodus für die Bearbeitung und die Anzeige ein- und ausschalten

Verwalten von geplanten Berichten

Sobald eine ausgewählte Berichtsdefinition für die Veröffentlichung *geplant* wurde, werden im rechten Bereich die folgenden interaktiven Schaltflächen und Tabellenspalten angezeigt.

Aktionen

- **Jetzt ausführen** – Führt einen bereits *geplanten* Bericht unverzüglich aus. Hiermit können Sie Berichte, für die eine Zeitüberschreitung aufgetreten ist, ein Fehler generiert wurde oder keine Genehmigung vorliegt, sofort erneut ausführen, ohne dass sämtliche Planungsoptionen nochmals gewählt werden müssen.
- **Neu planen** – Zeigt die Registerkarte **Planung** des Dialogfelds **Ausgewähltes Element neu planen** *(siehe 168)* an. Planen Sie auf dieser Registerkarte die Veröffentlichung eines ausgewählten Berichts neu. *Diese Optionen sind mit denen bei der ursprünglichen Planung eines Berichts identisch.*
- **Empfänger** – Zeigt die Registerkarte **Verteilung** des Dialogfelds **Ausgewähltes Element neu planen** *(siehe 168)* an. Ändern Sie auf dieser Registerkarte die Empfänger für einen ausgewählten Bericht, den Sie erneut planen. *Diese Optionen sind mit denen bei der ursprünglichen Planung eines Berichts identisch.*

- **Planung löschen** – Löscht einen ausgewählten veröffentlichten Bericht endgültig. Hierdurch wird nur der Datensatz des Berichts unter **Planung** *(siehe 163)* für Ihre VSA-Anmeldung gelöscht. Der Bericht wird jedoch *nicht* für andere Benutzer gelöscht.
- **Verlauf** – Hierdurch wird das Dialogfeld **Verlauf ausgewählter Elemente** aufgerufen, in dem alle veröffentlichten Instanzen eines empfangenen Berichts aufgeführt sind. Klicken Sie auf das Veröffentlichungsdatum des Berichts, den Sie anzeigen möchten, und klicken Sie dann unten im Dialogfeld auf den Hyperlink dieses Berichts.
- **Aktualisieren** – Aktualisiert die Seite.

Tabellenspalten

Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(siehe 18)*.

- **(Status)**
  - Anstehend
  - Abgeschlossen und Genehmigung erforderlich – Klicken Sie auf das Symbol , um den abgeschlossenen Bericht anzuzeigen und ihn dann zu genehmigen oder abzulehnen. Siehe **Genehmigen/Ablehnen von Berichten** *(siehe 171)*.
  - Abgeschlossen und abgelehnt – Klicken Sie auf das Symbol um den abgeschlossenen und abgelehnten Bericht anzuzeigen. Sie können ihn im Nachhinein noch genehmigen.
  - Abgeschlossen und verteilt – Klicken Sie auf das Symbol neben dem Namen des Berichts, um das Dialogfeld **Verlauf ausgewählter Elemente** mit dem Veröffentlichungsverlauf dieses Berichts anzuzeigen. Klicken Sie auf das Veröffentlichungsdatum des Berichts, den Sie anzeigen möchten, und klicken Sie dann unten im Dialogfeld auf den Hyperlink dieses Berichts.
  - Fehler – Der Bericht konnte nicht veröffentlicht werden.
- **Name** – Der Name des Berichts.
- **Eigentümer** – Der Ersteller des Berichts.
- **Wiederholung** – Klicken Sie auf die Wiederholung – `Einmal`, `Täglich`, `Wöchentlich`, `Monatlich` – um die Planung entsprechend zu aktualisieren.
- **Empfänger** – Klicken Sie auf die Anzahl von Empfängern, um die Liste der Empfänger im Dialogfeld **Ausgewähltes Element neu planen** *(siehe 168)* zu aktualisieren.
- **Empfängerliste** – Eine Liste von Empfängern
- **Zuletzt ausgeführt** – Die Zeit der letzten Veröffentlichung des Berichts
- **Nächster Durchlauf** – Die Zeit der nächsten geplanten Veröffentlichung des Berichts
- **Organisation, Rechnergruppe, Rechner, Ansicht** – Die **Datenfilter** *(siehe 168)*-Typen, mit denen die Daten in einem Bericht eingegrenzt werden. Verwenden Sie eine Ansicht, um mehr als eine Organisation, Rechnergruppe oder einen Rechner auszuwählen. Alle Rechnergruppen in allen Organisationen, die Sie gemäß Ihrem Scope anzeigen dürfen, sind standardmäßig ausgewählt.
- **Typ** – `Bericht` oder `Berichtsset`
- **Status** – Der Status des Berichts in Textformat
- **Ort** – Der Ordner, in dem der geplante Bericht sich befindet (mittlerer Fensterbereich)
- **Erstellungsdatum** – Das Datum, an dem der Bericht geplant war.
- **Scope** – Die Sichtbarkeit der Zeilen in der Tabelle 'Planung' wird durch den verwendeten Scope eingeschränkt. Ihr Scope muss mit dem Scope übereinstimmen, der bei der Planung des Berichts durch den Eigentümer aktuell war. Hierdurch wird sichergestellt, dass nur Benutzer, die zur Einsicht der gleichen im Bericht angezeigten Daten berechtigt sind, die Empfänger des Berichts neu planen und ändern können. E-Mail-Empfänger haben per E-Mail auf den abgeschlossenen Bericht immer Zugriff, selbst, wenn sie nicht Mitglieder des gleichen Scopes sind.

Genehmigen/Ablehnen von Berichten

Veröffentlichte Berichte können so konfiguriert werden, dass vor ihrer Verteilung an Empfänger eine Genehmigung erforderlich ist. Jeder Benutzer mit gemeinsamen Zugriffsrechten und dem gleichen Scope, der beim Erstellen des Berichts verwendet wurde, kann den veröffentlichten Bericht genehmigen oder ablehnen.

1. Aktivieren Sie in der Kopfzeile einer Berichtsdefinition das Kontrollkästchen **Genehmigung vor der Verteilung erforderlich**.
2. Planen Sie zum Erstellen eine veröffentlichten Berichts die Berichtsdefinition.
3. Warten Sie, bis für den Bericht das Statussymbol `Abgeschlossen und Genehmigung erforderlich` angezeigt wird.
4. Klicken Sie auf das Statussymbol, um das Dialogfeld **Verlauf geplanter Elemente** anzuzeigen.
5. Klicken Sie entweder auf die Schaltfläche **Bestätigen** oder **Ablehnen**.
   - Bestätigte Berichte werden an ihre Empfänger verteilt.
   - Abgelehnte Berichte werden mit dem Statussymbol `Abgeschlossen und abgelehnt` angezeigt. Optional können Sie zum Anzeigen des abgelehnten Berichts auf das Statussymbol klicken. Sie können ihn im Nachhinein noch genehmigen.

Benutzersicherheit bei Berichten und Berichtssets

Master-Benutzer

Master-Benutzer haben Zugriff auf beliebige Berichts- bzw. Berichtsset-Definitionen, vorausgesetzt, dass unter System > **Voreinstellungen** *(siehe 402)* das Kontrollkästchen **Freigegebene und private Ordnerinhalte aller Benutzer anzeigen** aktiviert ist. Der verbleibende Abschnitt unter diesem Thema bezieht sich auf die Zugriffsrechte von Benutzern, die *keine Master-Benutzer* sind.

Zugriff auf die Planung von Berichten und Berichtssets

Andere VSA-Benutzer können eine vom Eigentümer erstellte Berichts- bzw. Berichtsset-Definition unter den folgenden Voraussetzungen veröffentlichen oder neu planen:

- Der Ordner mit der Berichts- bzw. Berichtsset-Definition wurde ihnen freigegeben.
- Der aktuell ausgewählte Scope des VSA-Benutzers *entspricht dem Scope, der von dem Eigentümer zum Erstellen der Berichts- bzw. Berichtsset-Definition verwendet wurde*.

Wenn beide Bedingungen erfüllt sind, wird der geplante Bericht bzw. das geplante Berichtsset auf diesen Seiten angezeigt:

- **Planung** *(siehe 163)* – Zeigt *alle* geplanten Berichte und Berichtssets an, für die Sie Anzeigerechte besitzen.
- **Berichte** *(siehe 169)* – Zeigt alle geplanten Berichte für die ausgewählte Berichtsdefinition an, für die Sie Anzeigerechte besitzen.
- **Berichtssets** *(siehe 172)* – Zeigt alle geplanten Berichtssets für die ausgewählte Berichtsset-Definition an, für die Sie Anzeigerechte besitzen.

Eingang Empfänger

Nur VSA-Benutzer, deren Scope dem entspricht, der vom Eigentümer zum Erstellen der Berichts- oder Berichtsset-Definition verwendet wurde, können als **Eingang**-Empfänger eines Berichts bzw. Berichtssets bestimmt werden.

E-Mail-Empfänger

Selbst wenn der Scope eines Empfängers nicht dem Scope des Eigentümers zum Zeitpunkt der Erstellung des Berichts bzw. Berichtssets entspricht, können Empfänger Berichte und Berichtssets anzeigen, die ihnen als E-Mail-Empfänger zugeschickt wurden. Die veröffentlichten Berichte bzw. Berichtssets werden als E-Mail-Anhang geöffnet.

URL der Berichtskopfzeile festlegen

Standardmäßig zeigen VSA-Berichtskopfzeilen das unter "System > Seitenanpassung > **Website-Kopfzeile** *(siehe 448)*" angegebene Bild an. Durch Änderung des Werts in "System > Konfigurieren > **Berichtskonfiguration ändern** *(siehe 434)* > **Logo**" können Sie diese Standardeinstellung überschreiben und die URL *nur für Berichtskopfzeilen ändern*. Die Änderung der URL im Feld "Berichtskonfiguration ändern > **Logo**" wirkt sich nicht auf das Bild in der **Website-Kopfzeile** aus.

Berichtssets

Info Center > Reporting > Berichtssets

Ein **Berichtssatz** ist eine *Sammlung* von **Berichtsdefinitionen** *(siehe 165)*. Sie können eine *Berichtsset-Definition* genau wie eine einzelne *Berichtsdefinition* planen. Dies spart Ihnen den Umstand, Berichtsdefinitionen einzeln zu planen.

Einen Überblick über das Arbeiten mit Berichtssets erhalten Sie unter den folgenden Themen:

- **Berichtsset-Definitionen** *(siehe 172)*
- **Berichtsset-Ordnerstrukturen** *(siehe 173)*

Das Planen und Verwalten von geplanten *Berichtssets* verläuft in gleicher Weise wie das von geplanten *Berichten*. Siehe:

- **Planung/erneute Planung von Berichten** *(siehe 168)*
- **Datenfilter** *(siehe 168)*
- **Verwalten von geplanten Berichten** *(siehe 169)*
- **Genehmigen/Ablehnen von Berichten** *(siehe 171)*
- **Benutzersicherheit bei Berichten und Berichtssets** *(siehe 171)*

Berichtsset-Definitionen

Ein **Berichtssatz** ist eine *Sammlung* von **Berichtsdefinitionen** *(siehe 165)*. Sie können eine *Berichtsset-Definition* genau wie eine einzelne *Berichtsdefinition* planen. Dies spart Ihnen den Umstand, Berichtsdefinitionen einzeln zu planen.

Erstellen von neuen Berichtsset-Definitionen

Klicken Sie auf die Schaltfläche **Neues Berichtsset**, um eine neue Berichtsset-Definition zu erstellen. Im Dialogfeld **Neues Berichtsset** werden die folgenden Registerkarten angezeigt:

Allgemein

- **Allgemein** – Geben Sie den Namen und die Beschreibung des Berichtssatzes ein.
- **Nachricht** – Geben Sie die standardmäßig zu verwendende Betreffzeile und Nachricht ein, mit der Benutzer bei der Verteilung des Berichtssets benachrichtigt werden.

Berichte

- Aktivieren Sie die Berichtsdefinitionen, die Sie in die Berichtsset-Definition aufnehmen möchten.

Bearbeiten von vorhandenen Berichtsset-Definitionen

1. Klicken Sie in den **Berichtsset-Ordnerstrukturen** *(siehe 173)* im mittleren Bereich auf eine vorhandene Berichtsset-Definition.
2. Klicken Sie auf die Schaltfläche **Berichtsset bearbeiten**, um die Berichtsset-Definition zu bearbeiten. Im Dialogfeld **Berichtsset bearbeiten** werden dieselben Optionen wie im Dialogfeld **Neues Berichtsset** (siehe oben) angezeigt.

Anzeigen der Eigenschaften einer Berichtsset-Definition

1. Klicken Sie in den **Berichtsset-Ordnerstrukturen** *(siehe 173)* im mittleren Bereich auf eine vorhandene Berichtsset-Definition.
2. Sie können die Konfiguration der Berichtsset-Definition im rechten Bereich einsehen:
   - Im Abschnitt **Zugewiesene Berichte** der Registerkarte **Planung** werden die im Berichtsset enthaltenen Berichtsdefinitionen aufgeführt. Sie können in diesem Abschnitt Berichtsdefinitionen **zuweisen** oder **entfernen**.
   - Auf der Registerkarte **Allgemein** werden die standardmäßig zu verwendende Betreffzeile und Nachricht angezeigt, mit der Benutzer bei der Verteilung des Berichtssets benachrichtigt werden.

Berichtsset-Ordnerstrukturen

Berichtsdefinitionen werden mithilfe von zwei Ordnerstrukturen im mittleren Feld unterhalb der Cabinets **Privat** und **Gemeinsam nutzen** organisiert. Verwenden Sie die folgenden Optionen, um Objekte in diesen Ordnerstrukturen zu verwalten:

Immer verfügbar

- **(Filter anwenden)** – Geben Sie Text in das Bearbeitungsfeld des Filters ein und klicken Sie dann auf das Trichtersymbol , um das Filtern auf die Ordnerstrukturen anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in den Ordnerstrukturen gefunden wird.

Bei Auswahl eines Cabinets

- **Alle ausblenden** – Blendet alle Verzweigungen der Ordnerstruktur aus.
- **Alle erweitern** – Zeigt alle Verzweigungen der Ordnerstruktur an.

Bei Auswahl eines Ordners

- **Ordnereigenschaften** – Ordnereigenschaften werden im rechten Bereich angezeigt und führen den Eigentümer und die gültigen **Rechte** *(siehe 125)* für den Ordner auf.
- **Neu**
  - **Ordner** – Erstellt einen neuen Ordner unterhalb des ausgewählten Cabinets oder Ordners.
  - **Berichtsset** – Erstellt im ausgewählten Ordner der Ordnerstruktur eine neue **Berichtsset-Definition** *(siehe 172)* .
- **Löschen** – Löscht einen ausgewählten Ordner.
- **Umbenennen** – Benennt einen ausgewählten Ordner um.
- **Gemeinsam nutzen** – Dies gilt nur für **gemeinsam genutzte** genutzte Cabinet-Ordner. Hierdurch wird ein Ordner mit Benutzerrollen und einzelnen Benutzern freigegeben. Richtlinien zu den Freigaberechten für Objekte in Ordnerstrukturen finden Sie unter dem Thema **Ordnerrechte** *(siehe 125)*.

Bei Auswahl einer Berichtssatzdefinition

- **Neuer Berichtssatz** – Öffnet den Berichtseditor, um eine neue Berichtssatzdefinition im ausgewählten Ordner der Ordnerstruktur zu erstellen.
- **Bearbeiten** – Bearbeitet die ausgewählte Berichtsset-Definition.
- **Löschen** – Löscht die ausgewählte Berichtsset-Definition.
- **Planung** – Plant die Veröffentlichung der ausgewählten Berichtsset-Definition.

> **Hinweis:** Die Schaltfläche **Planung** ist möglicherweise für Standardbenutzer ausgeblendet. Diese Schaltfläche wird über den Knoten System > Systemvoreinstellungen > Planung aktivieren auf der Registerkarte **Benutzerrollen – Zugriffsrechte** *(siehe 415)* aktiviert.

Berichtsvorlagen

Info Center > Konfiguration und Design > Berichtsvorlagen

Über die Seite **Berichtsvorlagen** werden *anpassbare* Berichtsvorlagen definiert. Ausführlichere Informationen finden Sie unter:

- **Ordnerstruktur** *(siehe 176)*
- **Hinzufügen/Bearbeiten von Berichtsvorlagen** *(siehe 177)*
- **Histogramm** *(siehe 183)*
- **Tortendiagramm** *(siehe 186)*
- **Tabelle** *(siehe 179)*
- **Namenswert-Teil** *(siehe 189)*

Begriffe und Konzepte

- **Berichtsdefinitionen** – *Berichtsdefinitionen* enthalten alle Einstellungen für den Inhalt, das Layout und das Dateiformat eines Berichts. Ein Bericht wird basierend auf einer **Berichtsdefinition** *(siehe 165)* veröffentlicht.
- **Berichtsvorlagen** – Zur Erstellung einer Berichtsdefinition werden Einstellungen aus einer *Berichtsvorlage* kopiert. Berichtsdefinitionen enthalten alle *Standard*einstellungen für den Inhalt, das Layout und das Dateiformat einer Berichtsdefinition. Es gibt zwei Arten von Berichtsvorlagen:
  - **Benutzerdefiniert** – Anpassbare Berichtsvorlagen
  - **Legacy – In früheren Versionen bereitgestellte Berichtsvorlagen mit einem festgelegten Layout** *(siehe 203)*
- **Datasets** – Aus *Datasets* werden anpassbare Berichtsvorlagen erzeugt. Ein Dataset ist eine Sammlung von Daten, im Tabellenformat, die von der Kaseya Server SQL Server-Datenbank abgefragt wurden. Vordefinierte Datasets werden auf der Seite **Berichtsteile** *(siehe 192)*, organisiert nach VSA-Modulordnern, aufgelistet. Beispielsweise werden im Modulordner 'Agent' die folgenden Datasets zur Verfügung gestellt:

```
Agent Configuration
Agent Portal Access
Agent Protection Settings
Agent Status
```

- **Datenspalten** – Jedes Dataset ist eine Sammlung von einer oder mehreren *Datenspalte(n)*. Beispielsweise werden im Dataset `Agent-Status` die folgenden Datenspalten aufgelistet:

```
Agent-GUID
Rechnername
Aktueller Benutzer
Gruppenname
Letzter angemeldeter Benutzer
Rechner-ID
Online
Betriebssystem
Betriebssysteminformationen
   Reverse-Gruppenname
Quickinfo anzeigen
```

`Zeitzonenversatz`
`Quickinfo-Anmerkungen`
`Übergangszeit`

- **Berichtsteile** – Der Inhalt und das Layout einer Berichtsvorlage oder einer Berichtsdefinition setzt sich aus *Berichtsteilen* zusammen. Beim Erstellen eines *Berichtsteils* wählen Sie die Datenspalten in einem Dataset, die Sie in einer Berichtsvorlage oder Berichtsdefinition anzeigen möchten. *In jedem Teil können nur Datenspalten aus einem einzelnen Dataset ausgewählt werden.* Das Format der Anzeige von Daten hängt zudem von dem jeweiligen Berichtsteil ab. Es gibt vier Arten von *Berichtsteilformaten*:
  - **Tabellen** – Zeigt eine oder mehrere Spalte(n) mit Daten, die von dem ausgewählten Dataset zurückgegeben wurden, im Tabellenformat an.
  - **Balkendiagramme** – Zeigt ein Balkendiagramm basierend auf zwei Spalten mit Daten an, die von einem ausgewählten Dataset zurückgegeben wurden.
  - **Kreisdiagramme** – Zeigt ein Kreisdiagramm basierend auf zwei Spalten mit Daten an, die von einem ausgewählten Dataset zurückgegeben wurden.
  - **Namenswert-Teile** – Zeigt einen einzelnen Wert mit einer benutzerdefinierten Bezeichnung basierend auf einem *benutzerdefinierten* Dataset an. Zum Beispiel: `Open Tickets: 247`.

  Berichtsteil-Optionen – Jeder Berichtsteil kann anhand der folgenden Optionen konfiguriert werden:
  - **Aggregatoptionen** – Aggregatoptionen geben einen einzelnen *numerischen* Wert zurück, der sich aus mehreren Zellen in einer ausgewählten Spalte errechnet. Beispielsweise gibt die Aggregatoption `COUNT` die Anzahl der Werte ungleich null in einer ausgewählten Spalte zurück. Mit Ausnahme von `COUNT` bzw. `COUNT_BIG` werden Nullwerte von Aggregatfunktionen ignoriert.
  - **Ordnen nach** – Durch Kombination von ausgewählten Spalten, Aggregatoptionen und aufsteigenden bzw. absteigenden Sortierfolgen können Sie Daten in Ihrer bevorzugten Reihenfolge anzeigen.
  - **Gruppieren nach** – Zurückgegebene Datenzeilen können durch die Auswahl der Spalten 'Gruppieren nach' in Unterüberschriften und Untergruppen geordnet werden. Mehrere Ebenen von 'Gruppieren nach'-Spalten werden unterstützt. *Nur auf Tabellenabschnitte anwendbar.*
  - **Filtern** – Die angezeigten Daten können durch spezielle Datenfilter eingegrenzt werden. Dazu gehören:
    - ✓ Eine angegebene Anzahl von Zeilen oder ein Prozentsatz von Datenzeilen.
    - ✓ Vergleich ausgewählter Spalten mit bestimmten Werten.
- **Benutzerdefinierte Felder** – Benutzerdefinierte Agent-Felder – die über die Seiten Audit > **Rechnerübersicht** *(siehe 151)* oder **Systeminformationen** *(siehe 154)* erstellt wurden – werden in Ansichten, Verfahren, alten Berichten und **Berichtsteilen** *(siehe 192)* der ausgewählten Auditkategorie unterstützt. Benutzerdefinierte Berichte unterstützen höchstens 40 benutzerdefinierte Felder.
- **Deckblatt, Kopf-/Fußzeile** – Auf dieser **Seite** *(siehe 201)* werden die Darstellungselemente definiert, die unabhängig von den im Bericht angezeigten Daten sind. Sie können mithilfe dieser Elemente Ihren Berichten ein einzigartiges Erscheinungsbild und eine persönliche Note verleihen. Weisen Sie einzelnen benutzerdefinierten Berichtsvorlagen und Berichtsdefinitionen unterschiedliche Kombinationen von Deckblättern, Kopf- und Fußzeilen zu.
- **Veröffentlicht/Zurückgenommen** – Eine veröffentlichte Berichtsvorlage kann zur Erstellung von Berichtsdefinitionen verwendet werden. Zurückgenommen Berichtsvorlagen werden in der Liste der zur Erstellung von Berichtsdefinitionen verfügbaren Vorlagen ausgeblendet.
- **Als Vorlage festlegen** – Mit der Schaltfläche **Als Vorlage festlegen** unter **Berichte** wird eine Berichtsdefinition in einem ausgewählten Ordner namens **Berichtsvorlagen** gespeichert. Beispielsweise können Benutzer nützliche Verbesserungen für ihre eigenen Berichtsdefinitionen erstellen. Diese wiederum lassen sich in Berichtsvorlagen umwandeln, anhand derer andere Benutzer Berichtsdefinitionen erstellen können.

- **Teile erneut verwenden** – Jedes Mal, wenn ein Teil innerhalb einer Vorlage konfiguriert wird, können Sie das Teil optional auf der Seite **Berichtsteile** *(siehe 192)* speichern. Daraus entsteht ein sogenanntes 'Standardteil', das für Vorlagen und Berichtsdefinitionen erneut verwendet werden kann. Sie können auch ein Teil direkt aus einer bestehenden Vorlage in eine andere kopieren, ohne es als 'Standardteil' zu speichern.
- **Import/Export** – Sowohl Vorlagen als auch Berichtsteile können über System > **Import-Center** *(siehe 441)* im- und exportiert werden.

Ordnerstruktur

Info Center > Konfiguration und Design > Berichtsvorlagen

Berichtsvorlagen sind in einer einzelnen Ordnerstruktur im mittleren Bereich unterhalb der CAB-Datei **Vorlagen** abgelegt. Verwenden Sie die unten aufgeführten Optionen, um Berichtsvorlagen in dieser Ordnerstruktur zu verwalten.

> **Hinweis:** Die Kategorien, die Ihnen beim Erstellen einer neuen **Berichtsdefinition** *(siehe 165)* angezeigt werden, basieren auf den Ordnern der obersten Ebene in der Ordnerstruktur **Berichtsvorlagen** *(siehe 174)*. Standardmäßig wird ein Ordner der obersten Ebene für jedes installierte Modul erstellt.

Bei Auswahl der Vorlagen-CAB-Datei

- **Alle ausblenden** – Blendet alle Verzweigungen der Ordnerstruktur aus.
- **Alle erweitern** – Zeigt alle Verzweigungen der Ordnerstruktur an.

Bei Auswahl eines Ordners

Für jedes installierte Modul wurde ein Ordner erstellt. Sie können diese Ordner verwenden oder Ihren eigenen erstellen.

- **Ordner hinzufügen** – Fügt einen Berichtsvorlagenordner unter einem angegebenen Namen hinzu.
- **Hinzufügen** – Fügt im ausgewählten Ordner eine Berichtsvorlage hinzu.
- **Gemeinsam nutzen** – Gibt einen Ordner mit Benutzerrollen und einzelnen Benutzern frei. Richtlinien zu den Freigaberechten für Objekte in Ordnerstrukturen finden Sie unter dem Thema **Ordnerrechte** *(siehe 125)*.

Bei Auswahl einer Vorlage

- **Hinzufügen** – **Fügt** *(siehe 177)* im ausgewählten Ordner eine neue Berichtsvorlage hinzu.
- **Bearbeiten** – **Bearbeitet** *(siehe 177)* eine ausgewählte Berichtsdefinition.

> **Hinweis:** Systemberichtsvorlagen können zwar kopiert, jedoch weder bearbeitet noch gelöscht werden.

- **Löschen** – Löscht eine ausgewählte Berichtsvorlage.
- **Umbenennen** – Benennt eine ausgewählte Berichtsvorlage um.
- **Veröffentlichen/Zurücknehmen** – Schaltet den Veröffentlichungsstatus ein und aus. Durch Klicken auf **Veröffentlichen** aktivieren Sie eine Berichtsvorlage, die zum Erstellen einer **Berichtsdefinition** *(siehe 165)* verwendet werden kann. Durch Klicken auf **Zurücknehmen** wird verhindert, dass eine Berichtsvorlage zum Erstellen einer Berichtsdefinition verwendet wird.
- **Kopieren** – Erstellt eine Kopie einer vorhandenen Berichtsvorlage.
- **Vorschau** – Generiert einen Bericht nur für den aktuellen Benutzer basierend auf der ausgewählten Berichtsvorlage.

Hinzufügen/Bearbeiten von Berichtsvorlagen

Info Center > Konfiguration und Design > Berichtsvorlagen > Berichtsvorlage hinzufügen/Bearbeiten

Berichtsdesignbeschreibung

- **Name** – Der Name der Berichtsvorlage.
- **Vorlagentitel** – Der angezeigte Titel.

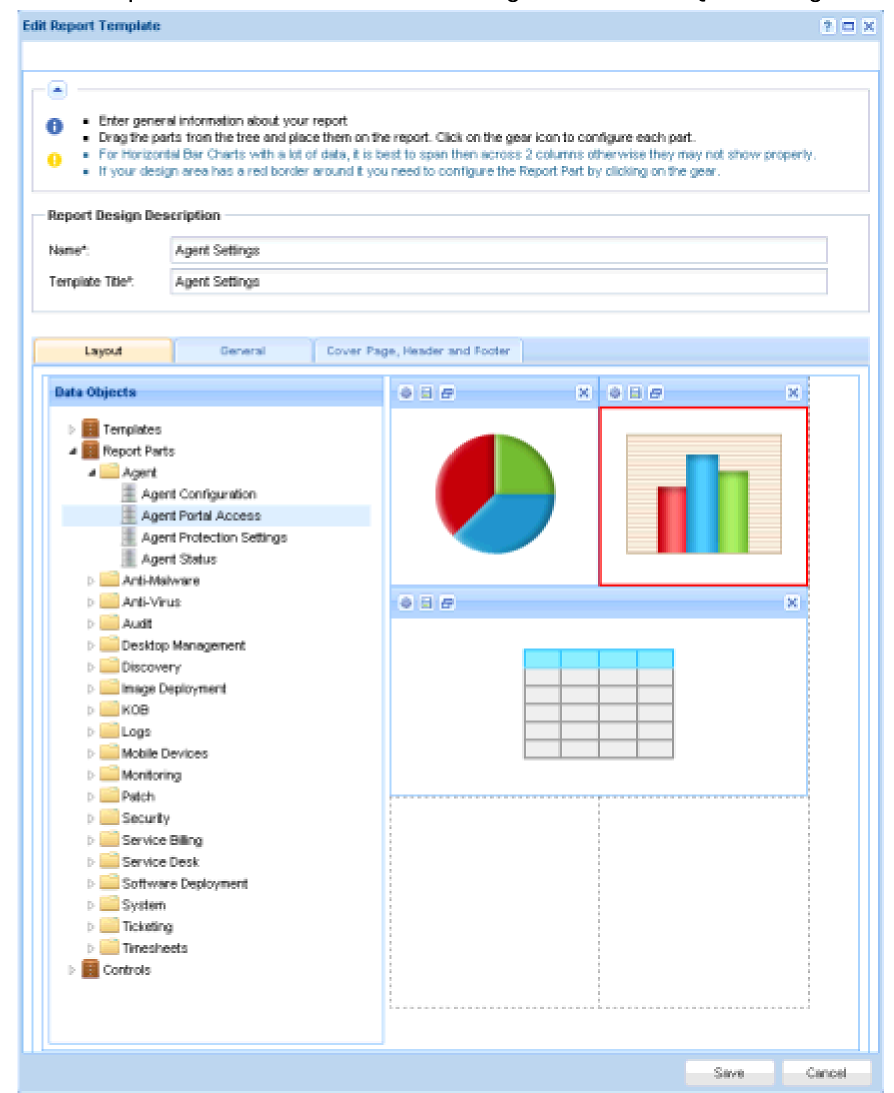
Hinweis: Unter **Berichtsdefinitionen** *(siehe 165)* finden Sie eine Beschreibung der Optionen auf den Registerkarten **Allgemein** und **Deckblatt, Kopf- und Fußzeile**.

Registerkarte Layouts

Im linken Bereich auf der Registerkarte **Layouts** wird eine Ordnerstruktur mit Datasets angezeigt. Im rechten Bereich wird eine Tabelle mit zwei Spalten angezeigt. Sie können Datasets aus der Ordnerstruktur in eine der Zellen der zweispaltigen Tabelle ziehen und ablegen. *Ein Dataset kann entweder nur eine oder beide Zelle(n) einer einzelnen Zeile belegen*. In einem Berichtsteil werden die von einem Dataset zurückgegebenen Daten in einem spezifischen Format angezeigt. Es gibt vier Arten von Berichtsteilformaten:

- **Tabellen** – Zeigt eine oder mehrere Spalte(n) mit Daten, die von dem ausgewählten Dataset zurückgegeben wurden, im Tabellenformat an.
- **Balkendiagramme** – Zeigt ein Balkendiagramm basierend auf zwei Spalten mit Daten an, die von einem ausgewählten Dataset zurückgegeben wurden.
- **Kreisdiagramme** – Zeigt ein Kreisdiagramm basierend auf zwei Spalten mit Daten an, die von einem ausgewählten Dataset zurückgegeben wurden.
- **Namenswert-Teile** – Zeigt einen einzelnen Wert mit einer benutzerdefinierten Bezeichnung basierend auf einem *benutzerdefinierten* Dataset an.

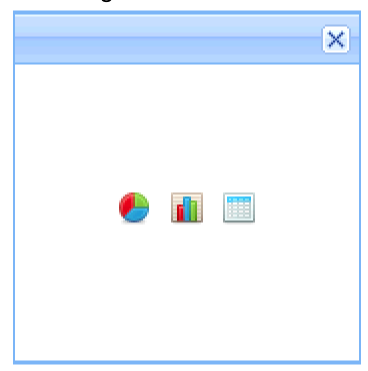
Eine Ordnerstruktur mit vorhandenen Vorlagen wird ebenfalls im linken Bereich angezeigt. Sie können ein Teil aus einer vorhandenen Vorlage in den rechten Bereich ziehen und ablegen und anschließend diese neue Kopie des Teils für Ihre neue Vorlage ändern. Die Quellvorlage bleibt unverändert.



Hinzufügen eines Berichtsteils zu einem Layout

1. Ziehen Sie ein Dataset aus der Ordnerstruktur im linken Bereich und legen Sie es in einer der Zellen im rechten Bereich ab.

2. Wählen Sie das Format für den Berichtsteil. Sie können nach Treffen dieser Auswahl nicht mehr zu einem anderen Format wechseln. Stattdessen können Sie den Berichtsteil löschen, neu hinzufügen und anschließend ein anderes Format wählen.



3. Klicken Sie auf das Zahnradsymbol oder doppelklicken Sie zum Konfigurieren des Berichtsteils auf die Zelle. Die Berichtsvorlage kann erst dann gespeichert werden, nachdem ein Berichtsteil zumindest einmal konfiguriert wurde. Die Zellen nicht konfigurierter Berichtsteile werden mit einer roten Umrandung angezeigt.



4. Die Konfiguration eines Berichtsteils hängt von der Art des ausgewählten Berichtsteils ab. Siehe:
   - **Tabelle** *(siehe 179)*
   - **Histogramm** *(siehe 183)*
   - **Tortendiagramm** *(siehe 186)*
   - **Namenswert-Teil** *(siehe 189)*
5. Verwenden Sie das Symbol zur Größenänderung , um ein Berichtsteil auf zwei Zellen in einer Zeile zu erweitern oder es zurück zu einer Einzelzelle zu reduzieren. *Die Erweiterung eines Berichtsteils in mehrere Zeilen wird nicht unterstützt.*
6. Jedes Mal, wenn ein Teil innerhalb einer Vorlage konfiguriert wird, können Sie das Teil optional auf der Seite **Berichtsteile** *(siehe 192)* speichern. Klicken Sie hierfür auf das Symbol zum Speichern . Hierdurch wird es zum 'Standardteil', das in Vorlagen und Berichtsdefinitionen verwendet werden kann.

Tabelle

Info Center > Konfiguration und Design > Berichtsvorlagen > Berichtsvorlage hinzufügen/Bearbeiten > Zahnradsymbol

Eine **Tabelle** wird mithilfe eines Drei-Schritte-Assistenten konfiguriert:

- Schritt 1 – Auswählen von Spalten
- Schritt 2 – Ordnen und Sortieren
- Schritt 3 – Filtern

Schritt 1 – Layout

Format

- **Dataset-Name** – Der Name des mit dieser Tabelle assoziierten Datasets.
- **Titel** – Geben Sie einen Titel für den Berichtsteil ein.
- **Titelausrichtung** – `Links`, `Rechts`, `Mitte`
- **Titel anzeigen** – Bei Aktivierung dieser Option wird der Titel im veröffentlichten Bericht mit diesem Berichtsteil angezeigt. Bei Deaktivierung wird der Titel ausgeblendet.
- **Seitenumbruch** – Bei Aktivierung dieser Option wird ein Seitenumbruch zum nächsten Berichtsteil erzwungen. Zu den Optionen gehören: `Kein Seitenumbruch`, `Vorher`, `Nachher`, `Vorher und nachher`. Ein Umbruch in einer der Zellen hat Vorrang vor der Zelle ohne Zeilenumbruch. Der Seitenumbruch `Nachher` wird ignoriert, wenn die Tabelle über die Seitenlänge hinaus in die andere Zelle verläuft.
- **Textgröße** – `Extra klein`, `Klein`, `Normal`, `Groß`.

Spalten und Spaltenauswahl

Ziehen Sie Spalten aus der Liste **Spalten** zur Liste **Spaltenauswahl** und legen Sie sie hier ab.

- **Zeile löschen** – Eine ausgewählte Spalte wird aus der Liste entfernt.
- **Spalte** – Eine Spalte, die für den Einschluss im veröffentlichten Bericht ausgewählt wurde.
- **Alias** – Zeigt einen Alias anstatt eines Spaltennamens als Überschrift für eine ausgewählte Spalte an.
- **Aggregat** – Aggregatoptionen geben einen einzelnen *numerischen* Wert zurück, der sich aus mehreren Zellen in einer ausgewählten Spalte errechnet. Beispielsweise gibt die Aggregatoption `COUNT` die Anzahl der Werte ungleich null in einer ausgewählten Spalte zurück. Mit Ausnahme von `COUNT` bzw. `COUNT_BIG` werden Nullwerte von Aggregatfunktionen ignoriert.
    - `AVG` – Gibt den Durchschnittswert in einer Gruppe zurück. Nullwerte werden ignoriert.
    - `COUNT / COUNT_BIG` – Gibt die Anzahl der Elemente in einer Gruppe zurück. Die Funktionsweise von `COUNT` und `COUNT_BIG` ist gleich. Der einzige Unterschied zwischen den beiden Funktionen besteht in den Rückgabewerten. `COUNT` gibt immer einen Wert vom Datentyp *int* zurück, `COUNT_BIG` dagegen einen Wert vom Datentyp *bigint*.
    - `MAX` – Gibt den Maximalwert in einer Gruppe zurück.
    - `MIN` – Gibt den Minimalwert in einer Gruppe zurück.
    - `STDEV` – Gibt die statistische Standardabweichung aller Werte in einer Gruppe zurück.
    - `STDEVP` – Gibt die statistische Standardabweichung für die Gesamtheit aller Werte in einer Gruppe zurück.
    - `SUM` – Gibt die Summe aller Werte in einer Gruppe zurück. SUM kann nur mit numerischen Spalten verwendet werden. Nullwerte werden ignoriert.
    - `VAR` – Gibt die statistische Varianz aller Werte in einer Gruppe zurück.
    - `VARP` – Gibt die statistische Varianz für die Gesamtheit aller Werte in einer Gruppe zurück.
- **Stellenwert** – Legt durch die Zuweisung eines numerischen Werts die prozentuale Breite jeder Spalte fest. Wenn beispielsweise vier Zeilen nacheinander mit den Werten 4, 3, 2, 1 gewichtet werden, dann gilt Folgendes:
    - Die erste Zeile mit einem Stellenwert von 4 macht 40 % der Summe aller gewichteten Werte (10) aus.
    - Die zweite Zeile mit einem Stellenwert von 3 macht 30 % der Summe aller gewichteten Werte (10) aus.
    - Die dritte Zeile mit einem Stellenwert von 2 macht 20 % der Summe aller gewichteten Werte (10) aus.

- Die vierte Zeile mit einem Stellenwert von 1 macht 10 % der Summe aller gewichteten Werte (10) aus.

Schritt 2 – Ordnen und Sortieren

Ordnen nach

Bestimmt die Reihenfolge, in der Daten angezeigt werden, vom ersten bis zum letzten Datenelement. Es können mehrere Zeilen konfiguriert werden, wobei eine höhere Zeile Vorrang gegenüber einer niedrigeren Zeile hat. Eine ausgewählte Reihenfolge nach Spalte muss im Bericht nicht angezeigt werden.

- **Zeile hinzufügen** – Fügt eine Ordnung nach Zeile hinzu.
- **Zeile löschen** – Löscht eine Ordnung nach Zeile.
- **Spalte** – Wählt eine Spalte aus, die die Reihenfolge zur Anzeige von Daten vom ersten bis zum letzten Datenelement bestimmt.
- **Aggregat** – Bei Auswahl einer Aggregatoption wird die Sortierfolge auf den von der Aggregatoption zurückgegebenen numerischen Wert anstand der ausgewählten Spalte angewendet. Lesen Sie die obigen Beschreibungen der einzelnen Aggregatoptionen.
- **Sortierfolge** – `Aufsteigend` oder `Absteigend`. Dies gilt entweder für die ausgewählte Spalte oder die Aggregatoption, falls eine angegeben wurde.

Gruppieren nach

Zurückgegebene Datenzeilen können durch die Auswahl der Spalten 'Gruppieren nach' in Unterüberschriften und Untergruppen geordnet werden. Mehrere Ebenen von 'Gruppieren nach'-Spalten werden unterstützt. Nur auf Tabellenabschnitte anwendbar.

- **Zeile hinzufügen** – Fügt eine Gruppe nach Zeile hinzu.
- **Zeile löschen** – Löscht eine Gruppe nach Zeile.
- **Spalte** – Die Spalte, die zum Gruppieren zurückgegebener Datenzeilen ausgewählt wird.

Schritt 3 – Filter

Die angezeigten Daten können durch spezielle Datenfilter eingegrenzt werden.

> **Hinweis:** Beim Ausführen oder Planen einer Berichtsdefinition oder Berichtsvorlage werden zusätzliche Filteroptionen angezeigt.

Zeilenfilter

- **Beschränkungstyp** – Der Typ der angegebenen Zeilenbeschränkung.
  - **Top N** – Begrenzt die zurückgegebenen Daten auf die ersten N Zeilen, die zurückgegeben werden. Beispiel: Wenn das **Limit** '10' lautet, werden die ersten 10 Zeilen von 300 verfügbaren Zeilen zurückgegeben. Ergebnis: 10 Zeilen werden zurückgegeben.
  - **Top N %** – Begrenzt die zurückgegebenen Daten auf die ersten N % von Zeilen, die zurückgegeben werden. Beispiel: Wenn das **Limit** '10' lautet, werden die ersten 10 % der Zeilen von 300 verfügbaren Zeilen zurückgegeben. Ergebnis: 30 Zeilen werden zurückgegeben.
- **Limit** – Die für das Feld **Beschränkungstyp** angegebene Anzahl.
- **Einzelne auswählen** – Bei Aktivierung dieser Option werden doppelte Zeilen nicht zurückgegeben. Bei allen in einem Bericht angezeigten Spalten müssen die Werte in einer Zeile mit den Werten in einer anderen Spalte übereinstimmen, um als Duplikat betrachtet zu werden.

Datumsfilter

Datumsfilter werden nur angezeigt, wenn Datum/Uhrzeit-Spalten im Berichtsteil enthalten sind.

- **Datumsfilterspalte** – Wählen Sie eine Datum/Uhrzeit-Spalte aus, um die in diesem Abschnitt des Berichts abgefragten Daten zu filtern.

Hinweis: Sie müssen eine Datum/Uhrzeit-Spalte auswählen, damit die anderen Datenfilteroptionen darunter eine Wirkung haben.

- **Zeitbereichstyp** – Wählen Sie eine Zeitspanne aus, um die in diesem Abschnitt des Berichts abgefragten Daten zu filtern.
  - Vordefinierte Bereiche – `Diese Woche`, `Letzte Woche`, `Dieser Monat`, `Letzter Monat`, `Dieses Quartal`, `Letztes Quartal`.
  - `Übernehmen von Bericht` – Wenn Sie einen Bericht planen oder ausführen, werden auf der Registerkarte **Filter** die Optionen **Datumsfilter** angezeigt. Diese bestimmen die Zeitspanne, in der für diesen Berichtsteil Datenabfragen erfolgen.
  - `Letzte N Tage` – Geben Sie den Wert `N` im Feld **Anzahl der Tage** ein.
  - `Festgelegter Bereich` – Geben Sie **Startdatum/-zeit** und **Enddatum/-zeit** ein.
- **Anzahl der Tage** – Geben Sie den Wert `N` in diesem Feld ein, wenn `Letzte N Tage` ausgewählt wurde.
- **Startdatum/-zeit** – Wählen Sie ein Startdatum und eine Startzeit, wenn `Festgelegter Bereich` ausgewählt wurde.
- **Enddatum/-zeit** – Wählen Sie ein Enddatum und eine Endzeit, wenn `Festgelegter Bereich` ausgewählt wurde.

Erweiterte Filter

Durch den Vergleich ausgewählter Spalten mit bestimmten Werten können Zeilen beschränkt werden.

- **Zeile hinzufügen** – Fügt eine Vergleichszeile hinzu.
- **Zeile löschen** – Löscht eine Vergleichszeile.
- **Feld** – Wählt eine Spalte aus, die zum Vergleich mit einem spezifischen Wert verwendet wird.
- **Operator**– Der Operator, der zum Vergleich einer ausgewählten Spalte mit einem bestimmten Wert verwendet wird.
  - `Gleich (=)` Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Nicht gleich (!=)` Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Wie` – Wenn eine ausgewählte Spalte diesen spezifischen Wert als Teilzeichenfolge enthält, wird diese Zeile angezeigt. Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Nicht wie` – Wenn eine ausgewählte Spalte nicht diesen spezifischen Wert als Teilzeichenfolge enthält, wird diese Zeile angezeigt. Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Greater Than (>)`
  - `Greater Than or Equal (>=)`
  - `Less Than (<)`
  - `Less Than Or Equal (<=)`
  - `Zwischen` – Wenn die ausgewählte Spalte sich zwischen zwei durch Kommas getrennten *Zeichenfolgenwerten* befindet, wird diese Zeile angezeigt. Der Vergleich erfolgt von links nach rechts. Beispiele:
    - ✓ Format des Zahlenfelds – `1000,9999`
    - ✓ Format des Zeichenfolgenfelds – `aaa,zzz`
    - ✓ Format des Datumsfelds – `01-01-2014,03-31-2014`
  - `Ist leer` – Falls die ausgewählte Spalte keine Zeichen enthält, wird diese Zeile angezeigt.

- ➢ `Ist Null` – Falls die ausgewählte Spalte null ist, wird diese Zeile angezeigt.
- ➢ `Nicht leer` – Falls die ausgewählte Spalte Zeichen enthält, wird diese Zeile angezeigt.
- ➢ `Nicht Null` – Falls die ausgewählte Spalte nicht null ist, wird diese Zeile angezeigt.
- **Wert** – Der angegebene Wert.

Histogramm

Info Center > Konfiguration und Design > Berichtsvorlagen > Berichtsvorlage hinzufügen/Bearbeiten > Zahnradsymbol

Ein **Histogramm** wird mithilfe eines Zwei-Schritte-Assistenten konfiguriert:

- Schritt 1 – Layout
- Schritt 2 – Filtern

Schritt 1 – Layout

Titel

- **Dataset-Name** – Der Name des mit dieser Tabelle assoziierten Datasets.
- **Titel in Bericht anzeigen** – Bei Aktivierung dieser Option wird der Titel im veröffentlichten Bericht mit diesem Berichtsteil angezeigt. Bei Deaktivierung wird der Titel ausgeblendet.
- **Titel** – Geben Sie einen Titel für den Berichtsteil ein.
- **Beschreibung** – Die Beschreibung eines Berichtsteils.

Format

- **Balkendiagrammtyp** – Die Ausrichtung und Form der Balken im Diagramm.
  - ➢ **Vertikaler Balken**
  - ➢ **Vertikaler Zylinderbalken**
  - ➢ **Horizontaler Balken**
  - ➢ **Horizontaler Zylinderbalken**

> **Hinweis:** Für horizontale Balkendiagramme ist es möglicherweise notwendig, dass die Daten in beiden Spalten des Berichtslayouts korrekt angezeigt werden.

- **Diagramm in 3D anzeigen** – Bei Aktivierung wird das Diagramm dreidimensional dargestellt. Die Darstellung von Zylinderbalkenoptionen muss dreidimensional sein.
- **Seitenumbruch** – Bei Aktivierung dieser Option wird ein Seitenumbruch zum nächsten Berichtsteil erzwungen. Zu den Optionen gehören: `Kein Seitenumbruch`, `Vorher`, `Nachher`, `Vorher und nachher`. Ein Umbruch in einer der Zellen hat Vorrang vor der Zelle ohne Zeilenumbruch. Der Seitenumbruch `Nachher` wird ignoriert, wenn die Tabelle über die Seitenlänge hinaus in die andere Zelle verläuft.
- **Achsentitel nicht anzeigen** – Bei Aktivierung werden Achsentitel nicht angezeigt.

Dateneigenschaften

- **Balkenkategorie** – Eine beliebige Spalte im Dataset, für die Sie unterschiedliche numerische Daten anzeigen möchten. Sie könnten z. B. für jede Rechnergruppe im veröffentlichen Bericht einen numerischen Wert anzeigen.
- **Balkenwert** – Jede weitere Spalte im Dataset, die sich numerisch darstellen lässt. **Ein Wert muss entweder numerisch sein oder als Ergebnis einer Aggregation numerisch bewertet werden.** Bei Auswahl einer *nicht-numerischen* Spalte können Sie nur `COUNT` oder `COUNT_BIG` als Aggregate verwenden.

- **Alias** – Zeigt einen Alias anstatt eines Spaltennamens als Überschrift für eine ausgewählte Spalte an.
- **Aggregat** – Aggregatoptionen geben einen einzelnen *numerischen* Wert zurück, der sich aus mehreren Zellen in einer ausgewählten Spalte errechnet. Beispielsweise gibt die Aggregatoption `COUNT` die Anzahl der Werte ungleich null in einer ausgewählten Spalte zurück. Mit Ausnahme von `COUNT` bzw. `COUNT_BIG` werden Nullwerte von Aggregatfunktionen ignoriert.
  - `AVG` – Gibt den Durchschnittswert in einer Gruppe zurück. Nullwerte werden ignoriert.
  - `COUNT / COUNT_BIG` – Gibt die Anzahl der Elemente in einer Gruppe zurück. Die Funktionsweise von `COUNT` und `COUNT_BIG` ist gleich. Der einzige Unterschied zwischen den beiden Funktionen besteht in den Rückgabewerten. `COUNT` gibt immer einen Wert vom Datentyp *int* zurück, `COUNT_BIG` dagegen einen Wert vom Datentyp *bigint*.
  - `MAX` – Gibt den Maximalwert in einer Gruppe zurück.
  - `MIN` – Gibt den Minimalwert in einer Gruppe zurück.
  - `STDEV` – Gibt die statistische Standardabweichung aller Werte in einer Gruppe zurück.
  - `STDEVP` – Gibt die statistische Standardabweichung für die Gesamtheit aller Werte in einer Gruppe zurück.
  - `SUM` – Gibt die Summe aller Werte in einer Gruppe zurück. SUM kann nur mit numerischen Spalten verwendet werden. Nullwerte werden ignoriert.
  - `VAR` – Gibt die statistische Varianz aller Werte in einer Gruppe zurück.
  - `VARP` – Gibt die statistische Varianz für die Gesamtheit aller Werte in einer Gruppe zurück.

Ordnen nach

Bestimmt die Reihenfolge, in der Daten angezeigt werden, vom ersten bis zum letzten Datenelement. Es können mehrere Zeilen konfiguriert werden, wobei eine höhere Zeile Vorrang gegenüber einer niedrigeren Zeile hat. Eine ausgewählte Reihenfolge nach Spalte muss im Bericht nicht angezeigt werden.

- **Zeile hinzufügen** – Fügt eine Ordnung nach Zeile hinzu.
- **Zeile löschen** – Löscht eine Ordnung nach Zeile.
- **Spalte** – Wählt eine Spalte aus, die die Reihenfolge zur Anzeige von Daten vom ersten bis zum letzten Datenelement bestimmt.
- **Aggregat** – Bei Auswahl einer Aggregatoption wird die Sortierfolge auf den von der Aggregatoption zurückgegebenen numerischen Wert anstand der ausgewählten Spalte angewendet. Lesen Sie die obigen Beschreibungen der einzelnen Aggregatoptionen.
- **Sortierfolge** – `Aufsteigend` oder `Absteigend`. Dies gilt entweder für die ausgewählte Spalte oder die Aggregatoption, falls eine angegeben wurde.

Schritt 2 – Filter

Die angezeigten Daten können durch spezielle Datenfilter eingegrenzt werden.

> **Hinweis:** Beim Ausführen oder Planen einer Berichtsdefinition oder Berichtsvorlage werden zusätzliche Filteroptionen angezeigt.

Zeilenfilter

- **Beschränkungstyp** – Der Typ der angegebenen Zeilenbeschränkung.
  - **Top N** – Begrenzt die zurückgegebenen Daten auf die ersten N Zeilen, die zurückgegeben werden. Beispiel: Wenn das **Limit** '10' lautet, werden die ersten 10 Zeilen von 300 verfügbaren Zeilen zurückgegeben. Ergebnis: 10 Zeilen werden zurückgegeben.
  - **Top N %** – Begrenzt die zurückgegebenen Daten auf die ersten N % von Zeilen, die zurückgegeben werden. Beispiel: Wenn das **Limit** '10' lautet, werden die ersten 10 % der

Zeilen von 300 verfügbaren Zeilen zurückgegeben. Ergebnis: 30 Zeilen werden zurückgegeben.

- **Limit** – Die für das Feld **Beschränkungstyp** angegebene Anzahl.
- **Einzelne auswählen** – Bei Aktivierung dieser Option werden doppelte Zeilen nicht zurückgegeben. Bei allen in einem Bericht angezeigten Spalten müssen die Werte in einer Zeile mit den Werten in einer anderen Spalte übereinstimmen, um als Duplikat betrachtet zu werden.

Datumsfilter

Datumsfilter werden nur angezeigt, wenn Datum/Uhrzeit-Spalten im Berichtsteil enthalten sind.

- **Datumsfilterspalte** – Wählen Sie eine Datum/Uhrzeit-Spalte aus, um die in diesem Abschnitt des Berichts abgefragten Daten zu filtern.

Hinweis: Sie müssen eine Datum/Uhrzeit-Spalte auswählen, damit die anderen Datenfilteroptionen darunter eine Wirkung haben.

- **Zeitbereichstyp** – Wählen Sie eine Zeitspanne aus, um die in diesem Abschnitt des Berichts abgefragten Daten zu filtern.
  - Vordefinierte Bereiche – `Diese Woche`, `Letzte Woche`, `Dieser Monat`, `Letzter Monat`, `Dieses Quartal`, `Letztes Quartal`.
  - `Übernehmen von Bericht` – Wenn Sie einen Bericht planen oder ausführen, werden auf der Registerkarte **Filter** die Optionen **Datumsfilter** angezeigt. Diese bestimmen die Zeitspanne, in der für diesen Berichtsteil Datenabfragen erfolgen.
  - `Letzte N Tage` – Geben Sie den Wert `N` im Feld **Anzahl der Tage** ein.
  - `Festgelegter Bereich` – Geben Sie **Startdatum/-zeit** und **Enddatum/-zeit** ein.
- **Anzahl der Tage** – Geben Sie den Wert `N` in diesem Feld ein, wenn `Letzte N Tage` ausgewählt wurde.
- **Startdatum/-zeit** – Wählen Sie ein Startdatum und eine Startzeit, wenn `Festgelegter Bereich` ausgewählt wurde.
- **Enddatum/-zeit** – Wählen Sie ein Enddatum und eine Endzeit, wenn `Festgelegter Bereich` ausgewählt wurde.

Erweiterte Filter

Durch den Vergleich ausgewählter Spalten mit bestimmten Werten können Zeilen beschränkt werden.

- **Zeile hinzufügen** – Fügt eine Vergleichszeile hinzu.
- **Zeile löschen** – Löscht eine Vergleichszeile.
- **Feld** – Wählt eine Spalte aus, die zum Vergleich mit einem spezifischen Wert verwendet wird.
- **Operator**– Der Operator, der zum Vergleich einer ausgewählten Spalte mit einem bestimmten Wert verwendet wird.
  - `Gleich (=)` Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Nicht gleich (!=)` Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Wie` – Wenn eine ausgewählte Spalte diesen spezifischen Wert als Teilzeichenfolge enthält, wird diese Zeile angezeigt. Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Nicht wie` – Wenn eine ausgewählte Spalte nicht diesen spezifischen Wert als Teilzeichenfolge enthält, wird diese Zeile angezeigt. Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Greater Than (>)`
  - `Greater Than or Equal (>=)`
  - `Less Than (<)`

  - `Less Than Or Equal (<=)`
  - `Zwischen` – Wenn die ausgewählte Spalte sich zwischen zwei durch Kommas getrennten *Zeichenfolgenwerten* befindet, wird diese Zeile angezeigt. Der Vergleich erfolgt von links nach rechts. Beispiele:
    - ✓ Format des Zahlenfelds – `1000,9999`
    - ✓ Format des Zeichenfolgenfelds – `aaa,zzz`
    - ✓ Format des Datumsfelds – `01-01-2014,03-31-2014`
  - `Ist leer` – Falls die ausgewählte Spalte keine Zeichen enthält, wird diese Zeile angezeigt.
  - `Ist Null` – Falls die ausgewählte Spalte null ist, wird diese Zeile angezeigt.
  - `Nicht leer` – Falls die ausgewählte Spalte Zeichen enthält, wird diese Zeile angezeigt.
  - `Nicht Null` – Falls die ausgewählte Spalte nicht null ist, wird diese Zeile angezeigt.
- **Wert** – Der angegebene Wert.

Tortendiagramm

Info Center > Konfiguration und Design > Berichtsvorlagen > Berichtsvorlage hinzufügen/Bearbeiten > Zahnradsymbol

Ein **Tortendiagramm** wird mithilfe eines Zwei-Schritte-Assistenten konfiguriert:

- Schritt 1 – Layout
- Schritt 2 – Filtern

Schritt 1 – Layout

Titel

- **Titel** – Geben Sie einen Titel für den Berichtsteil ein.
- **Titel in Bericht anzeigen** – Bei Aktivierung dieser Option wird der Titel im veröffentlichten Bericht mit diesem Berichtsteil angezeigt. Bei Deaktivierung wird der Titel ausgeblendet.

Format

- **Kreisdiagrammtyp** – Die Ausrichtung und Form der Balken im Diagramm.
  - **Standardkreisdiagramm**
  - **Aufgelöster Kreis**
- **Diagramm in 3D anzeigen** – Bei Aktivierung wird das Diagramm dreidimensional dargestellt.
- **Seitenumbruch** – Bei Aktivierung dieser Option wird ein Seitenumbruch zum nächsten Berichtsteil erzwungen. Zu den Optionen gehören: `Kein Seitenumbruch`, `Vorher`, `Nachher`, `Vorher und nachher`. Ein Umbruch in einer der Zellen hat Vorrang vor der Zelle ohne Zeilenumbruch. Der Seitenumbruch `Nachher` wird ignoriert, wenn die Tabelle über die Seitenlänge hinaus in die andere Zelle verläuft.
- **Wert innerhalb des Kreisdiagramms anzeigen** – Bei Aktivierung werden Werte innerhalb jedes Sektors des Kreis- bzw. Tortendiagramms angezeigt. Bei Deaktivierung dieser Option werden die Werte als Beschriftung um den Rand des Kreisdiagramms angezeigt.

Dateneigenschaften

- **Kategorie** – Eine beliebige Spalte im Dataset, für die Sie unterschiedliche numerische Daten anzeigen möchten. Sie könnten z. B. für jede Rechnergruppe im veröffentlichen Bericht einen numerischen Wert anzeigen.

- **Wert** – Jede weitere Spalte im Dataset, die sich numerisch darstellen lässt. **Ein Wert muss entweder numerisch sein oder als Ergebnis einer Aggregation numerisch bewertet werden.** Bei Auswahl einer *nicht-numerischen* Spalte können Sie nur `COUNT` oder `COUNT_BIG` als Aggregate verwenden.
- **Alias** – Zeigt einen Alias anstatt eines Spaltennamens als Überschrift für eine ausgewählte Spalte an.
- **Aggregat** – Aggregatoptionen geben einen einzelnen *numerischen* Wert zurück, der sich aus mehreren Zellen in einer ausgewählten Spalte errechnet. Beispielsweise gibt die Aggregatoption `COUNT` die Anzahl der Werte ungleich null in einer ausgewählten Spalte zurück. Mit Ausnahme von `COUNT` bzw. `COUNT_BIG` werden Nullwerte von Aggregatfunktionen ignoriert.
  - `AVG` – Gibt den Durchschnittswert in einer Gruppe zurück. Nullwerte werden ignoriert.
  - `COUNT / COUNT_BIG` – Gibt die Anzahl der Elemente in einer Gruppe zurück. Die Funktionsweise von `COUNT` und `COUNT_BIG` ist gleich. Der einzige Unterschied zwischen den beiden Funktionen besteht in den Rückgabewerten. `COUNT` gibt immer einen Wert vom Datentyp *int* zurück, `COUNT_BIG` dagegen einen Wert vom Datentyp *bigint*.
  - `MAX` – Gibt den Maximalwert in einer Gruppe zurück.
  - `MIN` – Gibt den Minimalwert in einer Gruppe zurück.
  - `STDEV` – Gibt die statistische Standardabweichung aller Werte in einer Gruppe zurück.
  - `STDEVP` – Gibt die statistische Standardabweichung für die Gesamtheit aller Werte in einer Gruppe zurück.
  - `SUM` – Gibt die Summe aller Werte in einer Gruppe zurück. SUM kann nur mit numerischen Spalten verwendet werden. Nullwerte werden ignoriert.
  - `VAR` – Gibt die statistische Varianz aller Werte in einer Gruppe zurück.
  - `VARP` – Gibt die statistische Varianz für die Gesamtheit aller Werte in einer Gruppe zurück.

Ordnen nach

Bestimmt die Reihenfolge, in der Daten angezeigt werden, vom ersten bis zum letzten Datenelement. Es können mehrere Zeilen konfiguriert werden, wobei eine höhere Zeile Vorrang gegenüber einer niedrigeren Zeile hat. Eine ausgewählte Reihenfolge nach Spalte muss im Bericht nicht angezeigt werden.

- **Zeile hinzufügen** – Fügt eine Ordnung nach Zeile hinzu.
- **Zeile löschen** – Löscht eine Ordnung nach Zeile.
- **Spalte** – Wählt eine Spalte aus, die die Reihenfolge zur Anzeige von Daten vom ersten bis zum letzten Datenelement bestimmt.
- **Aggregat** – Bei Auswahl einer Aggregatoption wird die Sortierfolge auf den von der Aggregatoption zurückgegebenen numerischen Wert anstand der ausgewählten Spalte angewendet. Lesen Sie die obigen Beschreibungen der einzelnen Aggregatoptionen.
- **Sortierfolge** – `Aufsteigend` oder `Absteigend`. Dies gilt entweder für die ausgewählte Spalte oder die Aggregatoption, falls eine angegeben wurde.

Schritt 2 – Filter

Die angezeigten Daten können durch spezielle Datenfilter eingegrenzt werden.

> **Hinweis:** Beim Ausführen oder Planen einer Berichtsdefinition oder Berichtsvorlage werden zusätzliche Filteroptionen angezeigt.

Zeilenfilter

- **Beschränkungstyp** – Der Typ der angegebenen Zeilenbeschränkung.
  - **Top N** – Begrenzt die zurückgegebenen Daten auf die ersten N Zeilen, die zurückgegeben werden. Beispiel: Wenn das **Limit** '10' lautet, werden die ersten 10 Zeilen von 300 verfügbaren Zeilen zurückgegeben. Ergebnis: 10 Zeilen werden zurückgegeben.

- Top N % – Begrenzt die zurückgegebenen Daten auf die ersten N % von Zeilen, die zurückgegeben werden. Beispiel: Wenn das **Limit** '10' lautet, werden die ersten 10 % der Zeilen von 300 verfügbaren Zeilen zurückgegeben. Ergebnis: 30 Zeilen werden zurückgegeben.

- **Limit** – Die für das Feld **Beschränkungstyp** angegebene Anzahl.
- **Einzelne auswählen** – Bei Aktivierung dieser Option werden doppelte Zeilen nicht zurückgegeben. Bei allen in einem Bericht angezeigten Spalten müssen die Werte in einer Zeile mit den Werten in einer anderen Spalte übereinstimmen, um als Duplikat betrachtet zu werden.

Datumsfilter

Datumsfilter werden nur angezeigt, wenn Datum/Uhrzeit-Spalten im Berichtsteil enthalten sind.

- **Datumsfilterspalte** – Wählen Sie eine Datum/Uhrzeit-Spalte aus, um die in diesem Abschnitt des Berichts abgefragten Daten zu filtern.

Hinweis: Sie müssen eine Datum/Uhrzeit-Spalte auswählen, damit die anderen Datenfilteroptionen darunter eine Wirkung haben.

- **Zeitbereichstyp** – Wählen Sie eine Zeitspanne aus, um die in diesem Abschnitt des Berichts abgefragten Daten zu filtern.
  - Vordefinierte Bereiche – `Diese Woche`, `Letzte Woche`, `Dieser Monat`, `Letzter Monat`, `Dieses Quartal`, `Letztes Quartal`.
  - `Übernehmen von Bericht` – Wenn Sie einen Bericht planen oder ausführen, werden auf der Registerkarte **Filter** die Optionen **Datumsfilter** angezeigt. Diese bestimmen die Zeitspanne, in der für diesen Berichtsteil Datenabfragen erfolgen.
  - `Letzte N Tage` – Geben Sie den Wert `N` im Feld **Anzahl der Tage** ein.
  - `Festgelegter Bereich` – Geben Sie **Startdatum/-zeit** und **Enddatum/-zeit** ein.
- **Anzahl der Tage** – Geben Sie den Wert `N` in diesem Feld ein, wenn `Letzte N Tage` ausgewählt wurde.
- **Startdatum/-zeit** – Wählen Sie ein Startdatum und eine Startzeit, wenn `Festgelegter Bereich` ausgewählt wurde.
- **Enddatum/-zeit** – Wählen Sie ein Enddatum und eine Endzeit, wenn `Festgelegter Bereich` ausgewählt wurde.

Erweiterte Filter

Durch den Vergleich ausgewählter Spalten mit bestimmten Werten können Zeilen beschränkt werden.

- **Zeile hinzufügen** – Fügt eine Vergleichszeile hinzu.
- **Zeile löschen** – Löscht eine Vergleichszeile.
- **Feld** – Wählt eine Spalte aus, die zum Vergleich mit einem spezifischen Wert verwendet wird.
- **Operator**– Der Operator, der zum Vergleich einer ausgewählten Spalte mit einem bestimmten Wert verwendet wird.
  - `Gleich (=)` Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Nicht gleich (!=)` Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Wie` – Wenn eine ausgewählte Spalte diesen spezifischen Wert als Teilzeichenfolge enthält, wird diese Zeile angezeigt. Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Nicht wie` – Wenn eine ausgewählte Spalte nicht diesen spezifischen Wert als Teilzeichenfolge enthält, wird diese Zeile angezeigt. Geben Sie eine durch Kommas getrennte Liste von Werten ein, um eine OR-Anweisung zu erstellen.
  - `Greater Than (>)`
  - `Greater Than or Equal (>=)`

- `Less Than (<)`
- `Less Than Or Equal (<=)`
- `Zwischen` – Wenn die ausgewählte Spalte sich zwischen zwei durch Kommas getrennten *Zeichenfolgenwerten* befindet, wird diese Zeile angezeigt. Der Vergleich erfolgt von links nach rechts. Beispiele:
  - ✓ Format des Zahlenfelds – `1000,9999`
  - ✓ Format des Zeichenfolgenfelds – `aaa,zzz`
  - ✓ Format des Datumsfelds – `01-01-2014,03-31-2014`
- `Ist leer` – Falls die ausgewählte Spalte keine Zeichen enthält, wird diese Zeile angezeigt.
- `Ist Null` – Falls die ausgewählte Spalte null ist, wird diese Zeile angezeigt.
- `Nicht leer` – Falls die ausgewählte Spalte Zeichen enthält, wird diese Zeile angezeigt.
- `Nicht Null` – Falls die ausgewählte Spalte nicht null ist, wird diese Zeile angezeigt.

- **Wert** – Der angegebene Wert.

Namenswert-Teil

Ein **Namenswertteil** ist ein Datenobjekttyp, der einer Berichtsvorlage oder Berichtsdefinition hinzugefügt werden kann. *Ein Namenswertteil zeigt einen einzelnen Wert zusammen mit einer benutzerdefinierten Bezeichnung* basierend auf einem *benutzerdefinierten* Dataset an. Diese benutzerdefinierten Datasets werden über die Seite **Namenswert-Teile** *(siehe 193)* definiert. So könnten Sie beispielsweise eine Liste mit einzelnen Werten für den Ticketstatus erstellen.

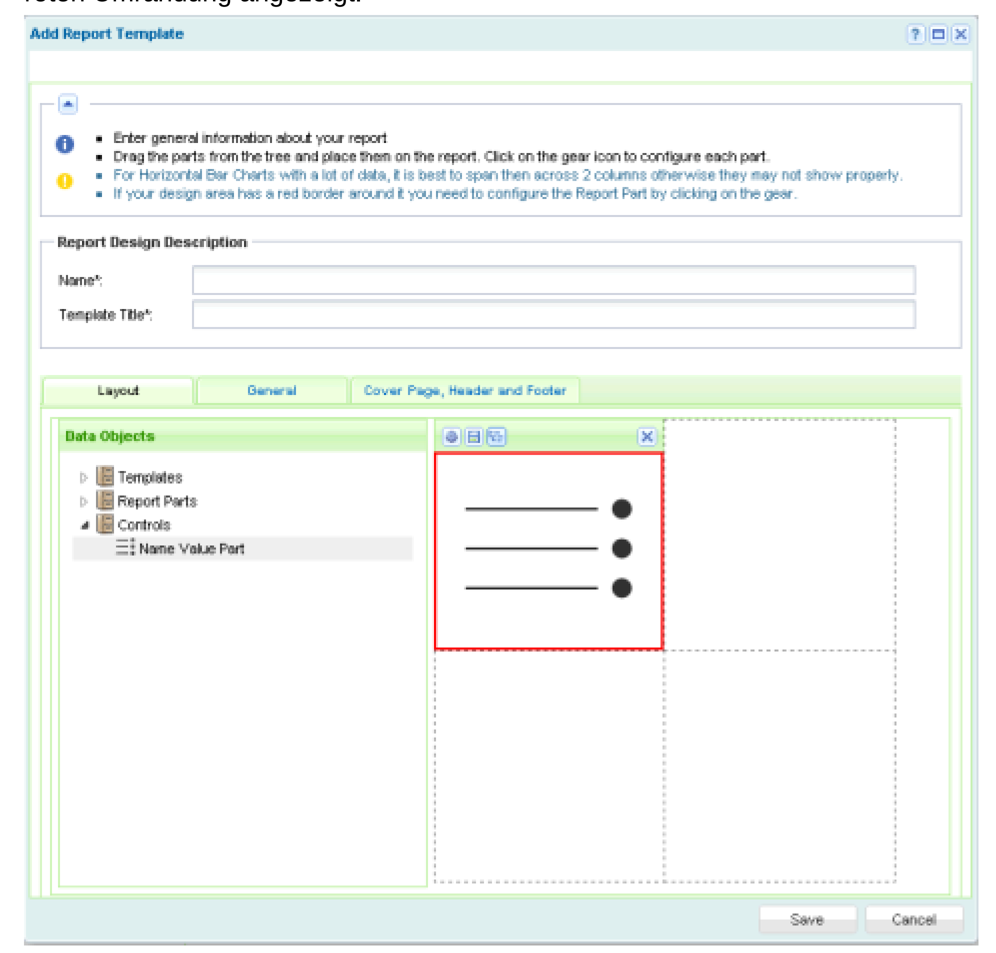
```
Tickets Created Last <N> Days
Total Tickets Past Due
Tickets Closed Last <N> Days
Total Open Tickets
```

> **Hinweis:** Das Erstellen oder Bearbeiten von Namenswert-Teilen wird nicht auf der Kaseya Cloud-Plattform unterstützt. Beim Erstellen einer Berichtsvorlage oder eines neuen benutzerdefinierten Berichts können für alle Cloud-basierten Konten vordefinierte Namenswert-Teile über die **Steuer**-CAB-Datei verwendet werden.

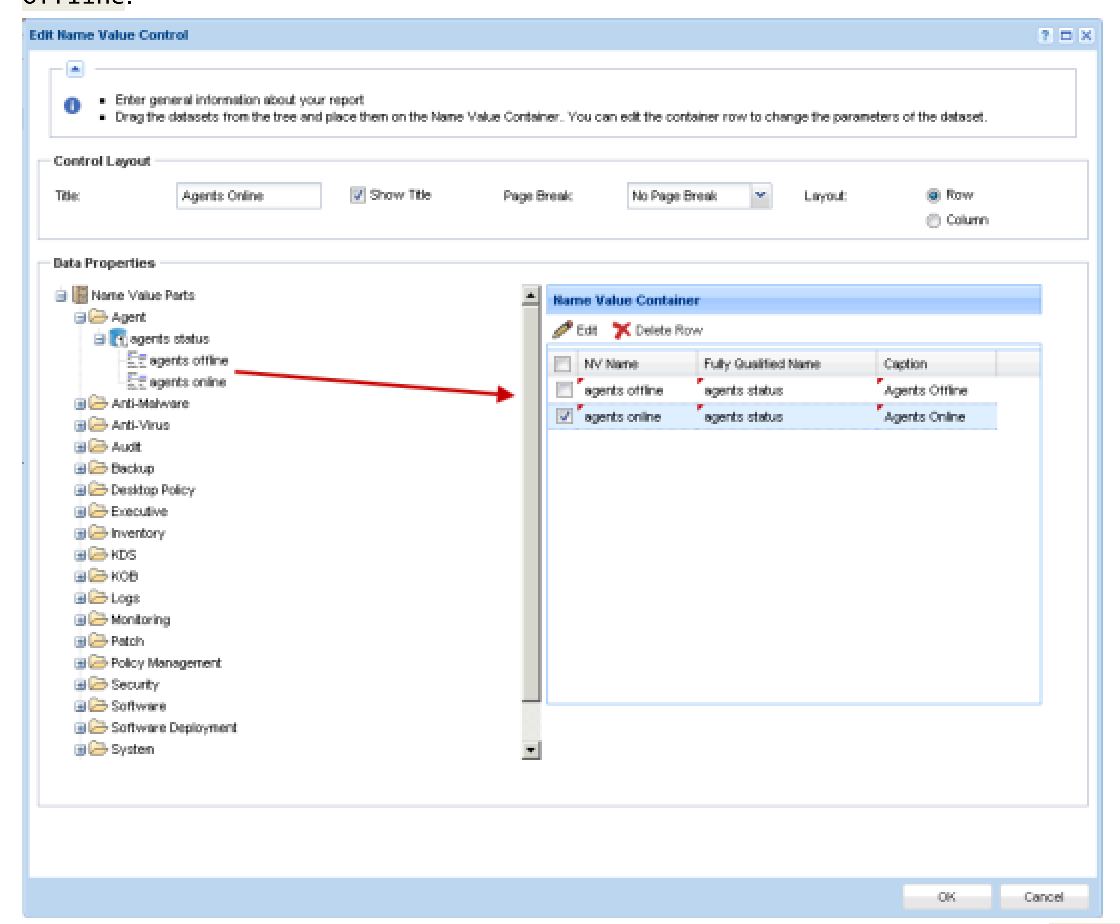
Hinzufügen eines Namenswert-Teils zu einem Layout

1. Ziehen Sie einen Namenswert-Teil aus der Ordnerstruktur im linken Bereich und legen Sie ihn in einer der Zellen im rechten Bereich ab.

2. Klicken Sie zum Konfigurieren des Namenswert-Teils auf das Zahnradsymbol ⚙. Die Berichtsvorlage kann erst dann gespeichert werden, nachdem ein Namenwert-Teil zumindest einmal konfiguriert wurde. Die Zellen nicht konfigurierter Namenswert-Teile werden mit einer roten Umrandung angezeigt.



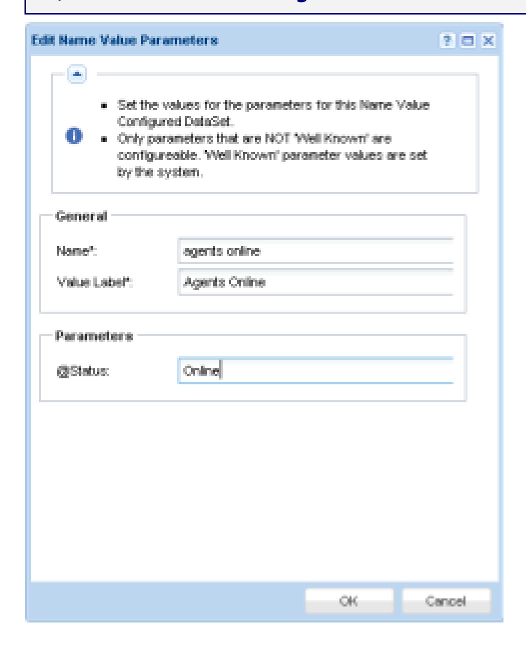
3. Ziehen Sie einen Namenswert-Teil aus der Ordnerstruktur im linken Bereich und legen Sie ihn in der Liste **Namenswert-Container** im rechten Bereich ab. Sie können mehrere Instanzen des gleichen Namenswert-Teils in derselben Liste ablegen. Beispielsweise kann eine **Namenswert-Container**-Liste folgende zwei Instanzen enthalten: `Agents Online` und `Agents Offline`.



Optional können Sie eine Instanz bearbeiten. Nehmen wir an, Sie möchten die Instanz `Agents Offline` in `Agents All` ändern.

4. Wählen Sie die Zeile der Instanz, die Sie bearbeiten möchten, aus der Liste **Namenswert-Container**.
5. Klicken Sie auf **Bearbeiten**. Jede Änderung, die Sie vornehmen, wird nur für diese Instanz in der Berichtsvorlage oder Berichtsdefinition, die Sie bearbeiten, übernommen.
   - **Name** – Der Name, der in Konfigurationsdialogen von dieser **Namenswert-Instanz** angezeigt wird.
   - **Namensbezeichnung** – Die Bezeichnung, die im Bericht mit ihrem entsprechenden Wert angezeigt wird.
   - **Parameter** – Ein oder mehrere Parameter, der/die beim Veröffentlichen eines Berichts den für diesen Namenswert-Teil zurückgegebenen Wert bestimmt/bestimmen. Die Werte, die ein Parameter einnehmen kann, hängen von der Abfrage oder dem gespeicherten Verfahren ab, die/das auf der Seite **Namenswert-Teile** *(siehe 193)* angegeben wird.

Hinweis: Bewegen Sie den Cursor über den Namen der einzelnen Parameter, um eine Quickinfo-Beschreibung der für diesen Parameter zulässigen Werte anzuzeigen.



Berichtsteile

Info Center > Konfiguration und Design > Berichtsteile

Auf der Seite **Berichtsteile** werden alle vordefinierten Datasets aufgelistet, die in benutzerdefinierten Berichten verwendet werden. Auf dieser Seite können Sie auch die Berichtsteile außerhalb einer Berichtsvorlage oder Berichtsdefinition konfigurieren. Über diese Seite definierte Berichtsteile liefern *standardmäßige Konfigurationen* für Berichtsteile, die Berichtsvorlagen und Berichtsdefinitionen hinzugefügt werden.

Hinweis: Eine Liste der in diesem Themenabschnitt verwendeten Begriffe und Konzepte finden Sie unter **Berichtsvorlagen** *(siehe 174)*.

Benutzerdefinierte Felder

Benutzerdefinierte Agent-Felder – die über die Seiten Audit > **Rechnerübersicht** *(siehe 151)* oder **Systeminformationen** *(siehe 154)* erstellt wurden – werden in Ansichten, Verfahren, alten Berichten und Berichtsteilen ausgewählter Auditkategorie unterstützt. Benutzerdefinierte Berichte unterstützen höchstens 40 benutzerdefinierte Felder.

Ordnerstruktur

In jedem Modulordner in der Ordnerstruktur wird/werden ein oder mehrere für dieses Modul angemessene Dataset(s) aufgelistet. Klicken Sie auf ein Dataset in der Ordnerstruktur, um die in diesem Dataset enthaltenen Spalten und Spaltenbeschreibungen anzuzeigen. Durch Klicken auf ein vorhandenen Berichtsteil wird im rechten Bereich seine aktuelle Konfiguration in Tabellenformat angezeigt.

Bei Auswahl der CAB-Datei

- **Alle ausblenden** – Blendet alle Verzweigungen der Ordnerstruktur aus.
- **Alle erweitern** – Zeigt alle Verzweigungen der Ordnerstruktur an.

Bei Auswahl eines Ordners

- Keine Aktionen stehen zur Verfügung.

Bei Auswahl eines Datasets

- **Neu** – Erstellt einen Berichtsteil basierend auf dem ausgewählten Dataset.
  - **Tabelle** – Fügt einen **Tabelle** *(siehe 179)*-Berichtsteil hinzu.
  - **Histogramm** – Fügt einen **Histogramm** *(siehe 183)*-Berichtsteil hinzu.
  - **Tortendiagramm** – Fügt einen **Tortendiagramm** *(siehe 186)*-Berichtsteil hinzu.

Bei Auswahl eines Berichtsteils

- **Neu** – Erstellt einen Berichtsteil basierend auf dem ausgewählten Dataset.
  - **Tabelle** – Fügt einen **Tabelle** *(siehe 179)*-Berichtsteil hinzu.
  - **Histogramm** – Fügt einen **Histogramm** *(siehe 183)*-Berichtsteil hinzu.
  - **Tortendiagramm** – Fügt einen **Tortendiagramm** *(siehe 186)*-Berichtsteil hinzu.
- **Bearbeiten** – Bearbeitet einen ausgewählten Berichtsteil.
- **Löschen** – Löscht einen ausgewählten Berichtsteil.
- **Umbenennen** – Benennt einen ausgewählten Berichtsteil um.
- **Vorschau** – Generiert eine Vorschau auf einen Berichtsteil.

Namenswert-Teile

Info Center > Konfiguration und Design > Namenswert-Teile

Über die Seite **Namenswert-Teile** wird ein benutzerdefiniertes Dataset erstellt, das zum Zeitpunkt der Veröffentlichung des Berichts einen einzelnen Wert aus der SQL-Datenbank zurückgibt. Der Wert wird mit einem benutzerdefinierten, aussagekräftigen Namen in einem Bericht angezeigt. Ein Namenwert-Teil namens `OnlineAgents` könnte z. B. eine einzige Zahl zurückgeben: die Anzahl aller Online-Agents, die den für den Bericht ausgewählten Filterkriterien entsprechen. Ausführlichere Informationen finden Sie unter:

- **Ordnerstruktur** *(siehe 194)*
- **Dataset hinzufügen/bearbeiten** *(siehe 194)*
- **Wohlbekannte Parameter** *(siehe 196)*
- **Berichtskontexte** *(siehe 199)*
- **Namenswert-Instanzen** *(siehe 201)*

> **Hinweis:** Das Erstellen oder Bearbeiten von Namenswert-Teilen wird nicht auf der Kaseya Cloud-Plattform unterstützt. Beim Erstellen einer Berichtsvorlage oder eines neuen benutzerdefinierten Berichts können für alle Cloud-basierten Konten vordefinierte Namenswert-Teile über die **Steuer-CAB**-Datei verwendet werden.

Begriffe und Konzepte

- **Namenswert-Steuerung** – Namenswert-Teile werden der CAB-Datei **Namenswert-Teil** *(siehe 189)* auf der Seite **Berichtsvorlagen** hinzugefügt. In jeder in einer Berichtsvorlage enthaltenen **Namenswert-Steuerung** kann ein Satz von **Namenswert-Teilen** im Zeilen- oder Spaltenformat dargestellt werden. Beispielsweise könnten Sie im Bericht einen Abschnitt namens `Ticketstatus` mit einer Reihe von Zahlenwerten erstellen, welche die Ticketanzahl für jeden der folgenden Namenswerte angeben:

```
Tickets erstellt während der letzten <N> Tage
Tickets überfällig gesamt
```

```
Tickets geschlossen während der letzten <N> Tage
Offene Tickets gesamt
```

- **Parameter** – Jedem Namenswert-Teil kann eine Anzahl von Parametern zugewiesen werden. Parameter müssen Standardargumente enthalten. Das Argument eines benutzerdefinierten Parameters wird beim Veröffentlichen des Berichts vom Benutzer eingegeben oder bestätigt.
- **Wohlbekannte Parameter** – Bestimmte Parameter sind dem System 'wohlbekannt' und müssen vom Benutzer beim Veröffentlichen des Berichts nicht definiert oder mit einem Argument versehen werden. Siehe **Wohlbekannte Parameter** *(siehe 196)*.
- **Namenswert-Instanz** – In einer Instanz werden die Argumente gespeichert, die den benutzerdefinierten Parametern eines benutzerdefinierten Datasets zugewiesen wurden. Diese Namenswert-Instanzen können einer Namenswert-Steuerung beigefügt werden, damit Argumente nicht jedes Mal, wenn eine Berichtsvorlage erstellt wird, manuell eingegeben werden müssen.

Ordnerstruktur

Info Center > Konfiguration und Design > Namenswert-Teile

Namenswert-Teile sind in einer einzelnen Ordnerstruktur im mittleren Bereich unterhalb der CAB-Datei **Namenswert-Teile** abgelegt. Verwenden Sie die unten aufgeführten Optionen, um Namenswert-Teile in dieser Ordnerstruktur zu verwalten.

Bei Auswahl der CAB-Datei für Namenswert-Teile

- **Alle ausblenden** – Blendet alle Verzweigungen der Ordnerstruktur aus.
- **Alle erweitern** – Zeigt alle Verzweigungen der Ordnerstruktur an.

Bei Auswahl eines Ordners

Für jedes installierte Modul wurde ein Ordner erstellt. Sie können diese Ordner verwenden oder Ihren eigenen erstellen.

- **Neues Dataset** – **Fügt** *(siehe 194)* ein benutzerdefiniertes Dataset in den ausgewählten Ordner ein.

Bei Auswahl eines Datasets

- **Dateset bearbeiten** – **Bearbeitet** *(siehe 194)* ein ausgewähltes Dataset.
- **Namenswert-Instanz hinzufügen** – Fügt im ausgewählten Ordner eine Namenswert-Instanz hinzu.
- **Löschen** – Löscht ein benutzerdefiniertes Dataset.

Bei Auswahl einer Namenswert-Instanz

- **Bearbeiten** – Bearbeitet eine Namenswert-Instanz.
- **Löschen** – Löscht eine Namenswert-Instanz.

Dataset hinzufügen/bearbeiten

Info Center > Konfiguration und Design > Namenswert-Teile > Neues Dataset oder Dataset bearbeiten

Im Fenster **Neues Dataset** oder **Dataset bearbeiten** wird das benutzerdefinierte Dataset angegeben, mit dem ein einzelner Wert aus der SQL-Datenbank zurückgegeben wird. Das benutzerdefinierte Dataset verwendet entweder eine SQL-SELECT-Anweisung oder ein gespeichertes Verfahren zur Rückgabe von Daten. Der von der ersten Datenzeile zurückgegebene Wert in einer ausgewählten Spalte ist der im Bericht aufgeführte Wert.

Aktion

- **Register-Datei erstellen** – Nachdem Sie über diesen Dialog ein Namenswert-Teil hinzugefügt oder bearbeitet haben:

1. Klicken Sie auf **Register-Datei erstellen**. In der nachfolgenden Dialogseite wird ein Link zu einer generierten Dataset-XML angezeigt.
2. Laden Sie die Dataset-XML herunter und legen Sie sie unter dem folgenden Pfad ab: `\<KServerInstallDirectory>\Xml\Reporting\Custom\DataSetRegistration\1`
3. Klicken Sie auf System > Serververwaltung > Konfigurieren > **Berichtserstellung-Konfiguration ändern** *(siehe 434)* > **Registrierung ausführen**, um die neue oder bearbeitete Dataset-XML bei Ihrem VSA zu registrieren.

Eigenschaften

- **Name** – Der Name des benutzerdefinierten Datasets.
- **Beschreibung** – Eine längere Beschreibung des benutzerdefinierten Datasets.
- **Kategorie** – Der Ordner **Namenswert-Teile**, der normalerweise dem Modul entspricht, in dem sich das benutzerdefinierte Dataset befindet.

SQL-Definition

- **Rückgabespalte** – Die Datenspalte in der SQL-SELECT-Anweisung, die den im veröffentlichten Bericht verwendeten Wert enthält. Der Wert in der ersten zurückgegebenen Datenzeile wird verwendet.
- **Titel** – Der Titel, der mit dem Wert im veröffentlichten Bericht angezeigt wird.
- **Datentyp** – Der zurückgegebene Datentyp. Dieser Datentyp muss mit dem Datentyp der Datenspalte in der SQL-SELECT-Anweisung kompatibel sein.
  - `STRING`
  - `INT`
  - `DECIMAL`
  - `DATE`
  - `BOOLEAN`
- **Zusammenhang** – Legt den Filtertyp fest, der kurz vor dem Generieren des Berichts angezeigt wird. Der Zusammenhang muss mit den von der SQL-Definition zurückgegebenen Daten kompatibel sein. Wenn z. B. die von der SQL-Definition zurückgegebenen Daten hauptsächlich nach Agent-Rechner durchgeführte Filterung unterstützen, dann sollte der ausgewählte Zusammenhang auf `MachineFilter` gesetzt werden.
  - `MachineFilter`
  - `ServiceDeskFilter`
  - `AssetsFilter`
  - `DevicesFilter`
  - `MobileDevicesFilter`
  - `TicketingFilter`
- **Text** – Eine SQL-SELECT-Anweisung, mit der eine oder mehrere Datenspalte(n) zurückgegeben werden. Nur die erste von der SQL-SELECT-Anweisung zurückgegebene Datenzeile wird verwendet.
- **Gespeichertes Verfahren** – Der Name eines gespeicherten Verfahrens oder beliebiger benutzerdefinierter Parameter. Nur die erste von dem gespeicherten Verfahren zurückgegebene Datenzeile wird verwendet.

Parameter

Durch eine SQL-SELECT-Anweisung oder ein gespeichertes Verfahren angegebene benutzerdefinierte Parameter müssen hier registriert werden. Dadurch können diese Parameter in den Konfigurationsdialogen von Berichtsvorlagen oder Namenwert-Teilen angezeigt werden.

Aktionen

- **Zeile hinzufügen** – Fügt eine Parameterzeile hinzu.
- **Zeile löschen** – Löscht eine ausgewählte Parameterzeile.

Spalten

- **Parametername** – Der Name des Parameters.
- **Parameterwert** – Der Standardwert für den Parameter.
- **Parametertyp** – Der Datentyp des Parameters.
  - `STRING`
  - `INT`
  - `DECIMAL`
  - `DATE`
  - `BOOLEAN`
- **Größe** – Die Größe des Parameters.
- **Beschreibung** – Geben Sie eine Beschreibung der zulässigen, von diesem Parameter unterstützten Werte ein. Bei der Auswahl eines anderen Werts für einen Parameter können Benutzer auf diese Beschreibung zugreifen, indem sie den Cursor über den Parameternamen bewegen und dessen Quickinfo anzeigen.

Wohlbekannte Parameter

Beim Erstellen von Namenswert-Teilen können Sie in Ihre Abfragen **wohlbekannte** Parameter mit aufnehmen. Sie fügen diese mittels des Formats `@<wellknownname>` in SQL-Abfragen ein. Außerdem müssen Sie sie in die Parametertabelle einfügen. Nachstehend sind wohlbekannte Werte aufgeführt, die Sie verwenden können:

- `@LogoURL` – Die URL zum im Bericht verwendeten Logo.
- `@ViewID` – Die ID für die Ansicht, die beim Erstellen des Berichts ausgewählt wurde, bzw. -1.
- `@AdminID` – Die ID des VSA-Benutzers, der den Bericht ausführt.
- `@CompanyName` – Der für MyOrg festgelegte Organisationsname.
- `@EffectiveDate` – Das Datum, an dem der Bericht ausgeführt wird (an die Zeitzone angepasst).
- `@PartitionID` – Die ID der Partition, in der der Bericht ausgeführt wird.
- `@ReportDate` – Das Datum, an dem der Bericht ausgeführt wird (an die Zeitzone angepasst).
- `@ReportTitle` – Der Titel des Berichts, der bei der Erstellung des Berichts festgelegt wurde.
- `@ScopeID` – Die ID des Scope, unter dem der Bericht ausgeführt wird.
- `@RoleID` – Die ID der Rolle, unter der der Bericht ausgeführt wird.
- `@ReportSessionId` – Die ID, die für das Ausführen des Berichts verwendet wird. Über diese ID wird eine JOIN-Verknüpfung zu einer ausgewählten **Kontext** *(siehe 199)*-Tabelle hergestellt. Bei der Verwendung von `@ReportSessionId` *muss* ein Kontext aus der Dropdown-Liste ausgewählt werden.
- `@LangID` – Die ID der Sprache, die für den Bericht verwendet wird.
- `@StartDateTime` – Ein spezieller Datumsparameter, mit dem Sie in Verbindung mit `@EndDateTime` zum Zeitpunkt der Berichtsausführung einen Datumsbereich auswählen können.
- `@EndDateTime` – Ein spezieller Datumsparameter, mit dem Sie in Verbindung mit `@StartDateTime` zum Zeitpunkt der Berichtsausführung einen Datumsbereich auswählen können.

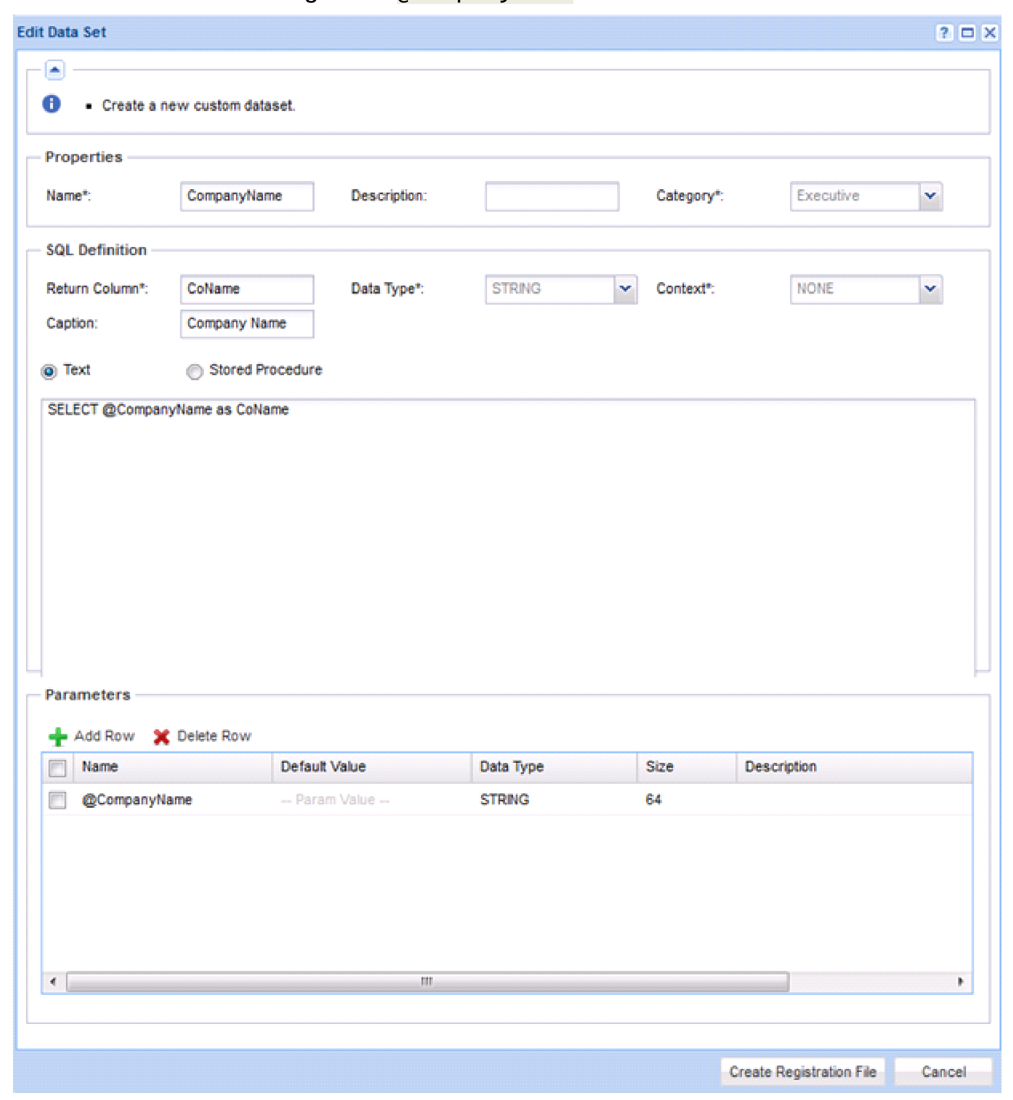
ReportSessionID

Wenn Sie einen Kontext verwenden, dann nehmen Sie den Parameter `@ReportSessionId` als Wert für einen der Parameter mit auf.

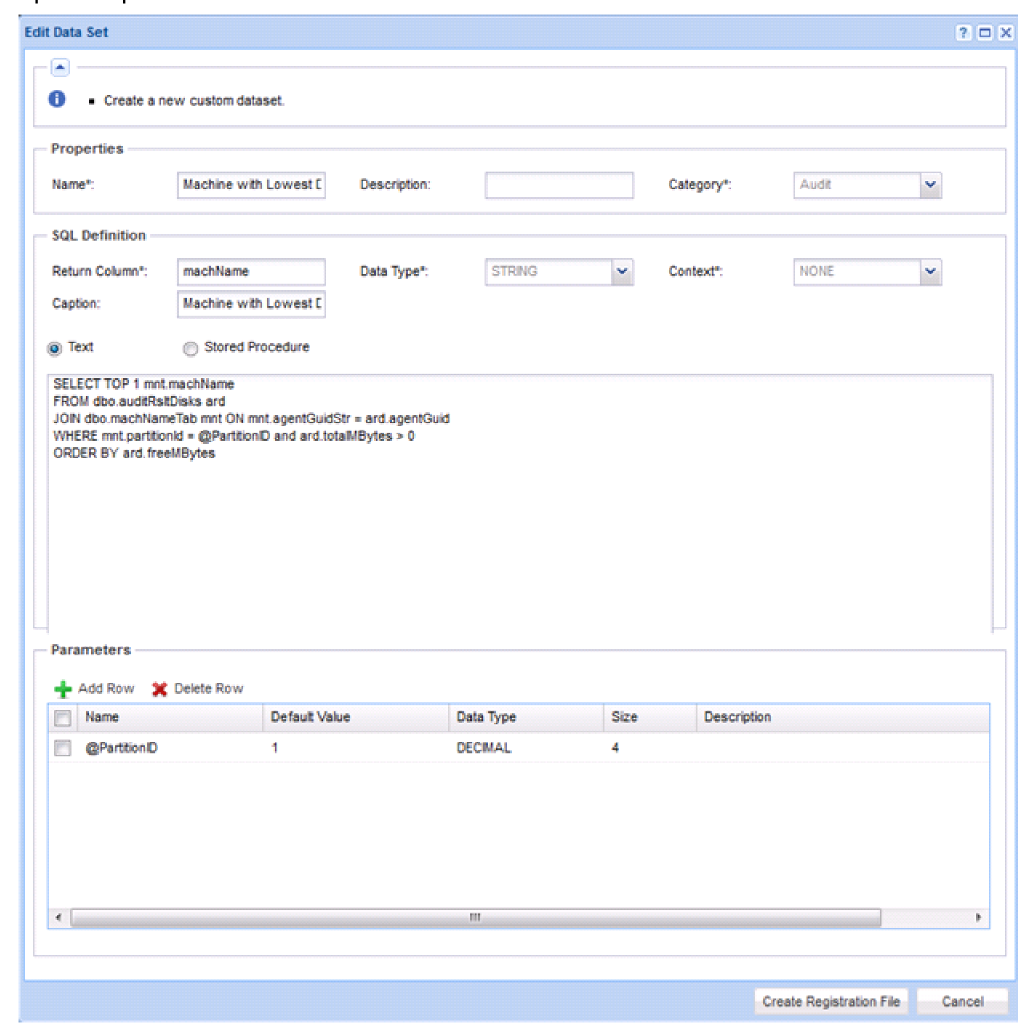
Beispiele

Hier sind einige Beispiele dafür, wie Namenswert-Teile mithilfe von wohlbekannten Parametern erzeugt werden.

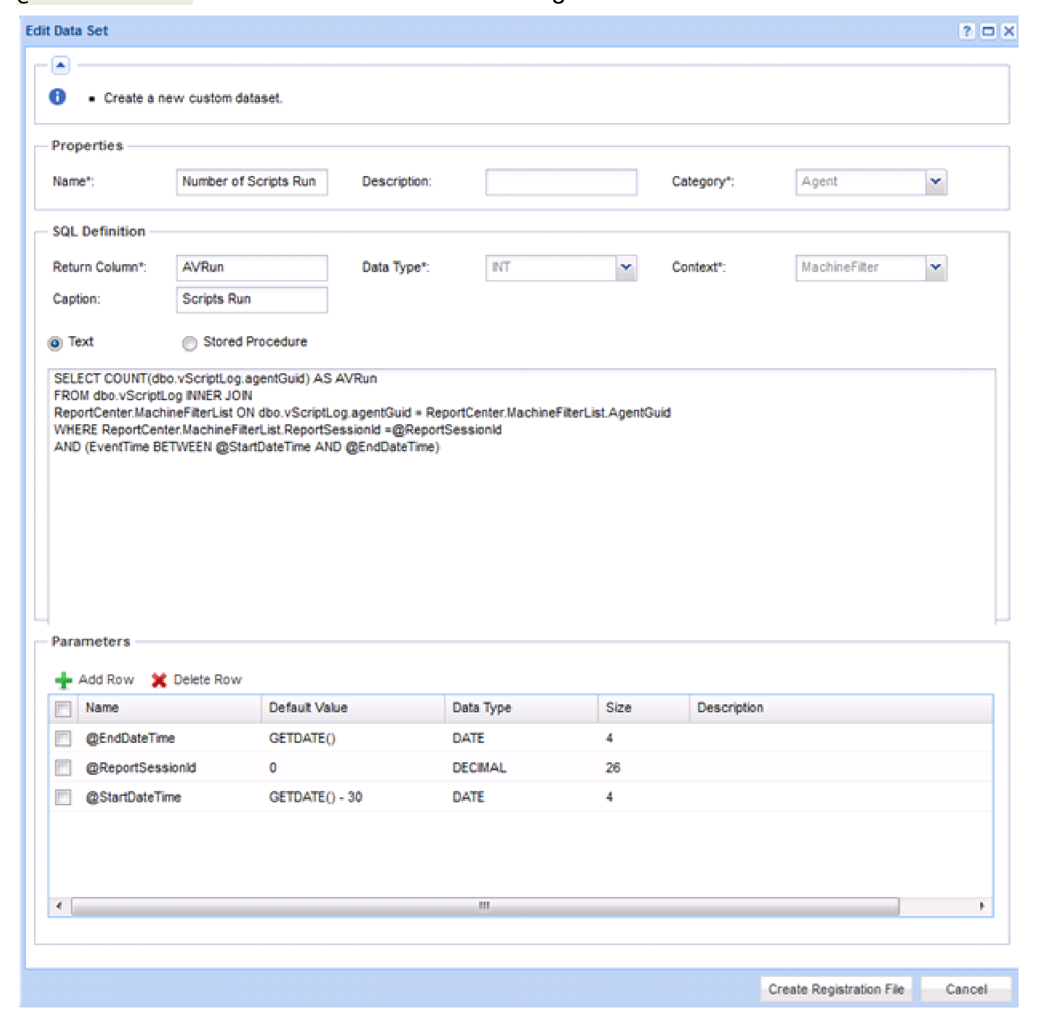
1. Dieser Namenswert-Teil gibt mit `@CompanyName` den Unternehmensnamen zurück.



2. Dieser Namenswert-Teile gibt mit `@PartitionID` den Rechner zurück, der den wenigsten Speicherplatz in der Partitions-ID hat.



3. Dieser Namenswert-Teil verwendet den Parameter `@ReportSessionID` , um die Anzahl der ausgeführten Agent-Verfahren zurückzugeben. Über den **Kontext** *(siehe 199)* MachineFilter können Sie beim Ausführen des Berichts Filter auswählen. Über die Parameter `@StartDateTime` und `@EndDateTime` können Sie bei der Ausführungszeit einen Datumsbericht auswählen.



Berichtskontexte

Beim Ausführen einer Berichtsdefinition oder bei der Vorschau auf einen Berichtsteil oder eine Berichtsvorlage können Sie mittels **Berichtskontexten** Filter auf Ihre Datasets anwenden. Jeder Kontext stellt unterschiedliche Filter zur Verfügung. Mit einem Filter wird eine temporäre Tabelle mit einer Liste von Elementen gefüllt, die Sie mit JOIN verknüpfen können. Dies wiederum begrenzt die Anzahl der Rückgabewerte bei Ihrer Abfrage.

In der folgenden Tabelle werden die verfügbaren Berichtskontexte, die für jeden Kontext verwendete temporäre Tabelle sowie die Spalte aufgeführt, zu der eine JOIN-Verknüpfung hergestellt werden kann.

Name	TableName	Spalte
MachineFilter	ReportCenter.MachineFilterList	AgentGuid
ServiceDeskFilter	ReportCenter.IncidentsFilterList	IncidentId

AssetsFilter	ReportCenter.AssetsFilterList	AssetId
DevicesFilter	ReportCenter.DevicesFilterList	DeviceId
MobileDevicesFilter	ReportCenter.MobileDevicesFilterList	DeviceId
TicketingFilter	ReportCenter.TicketingFilterList	TicketId

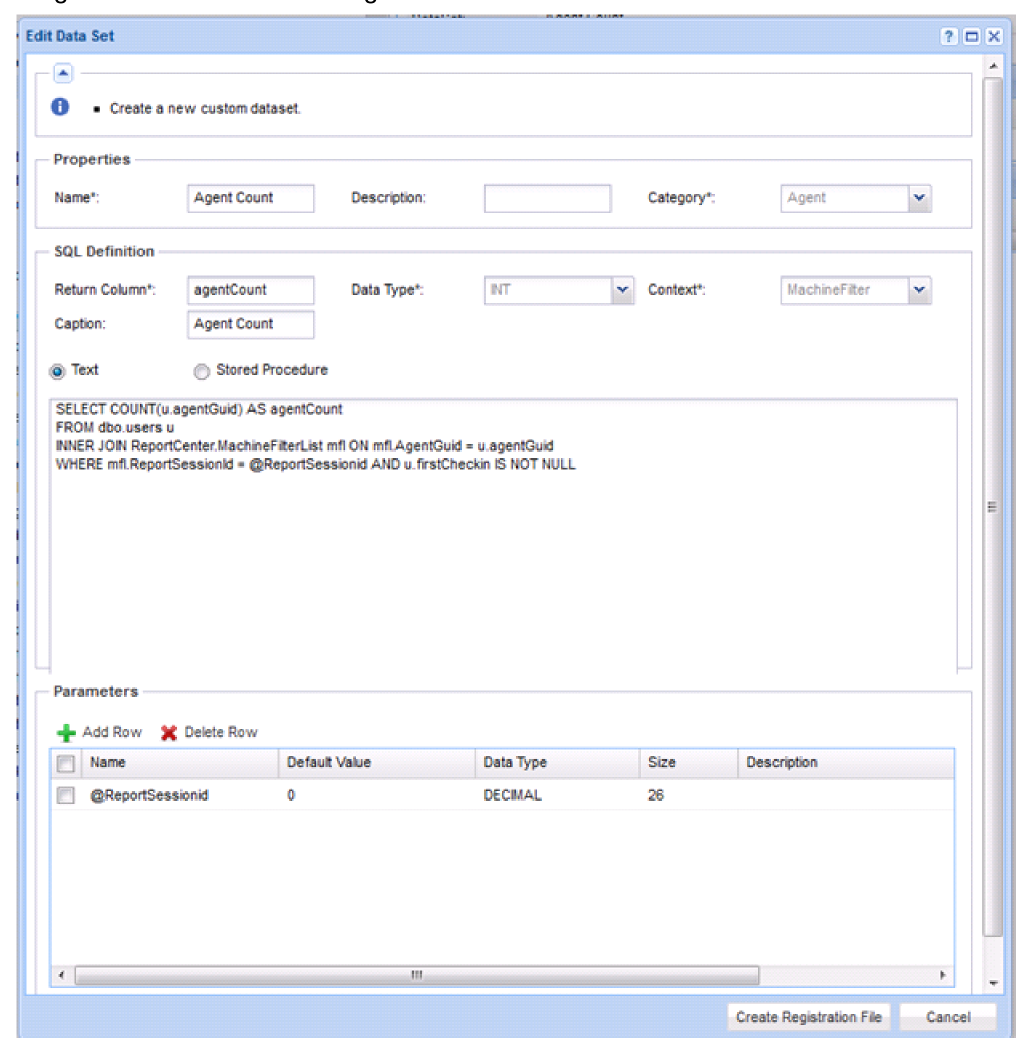
Ihre Abfrage sollte sowohl eine JOIN-Verknüpfung zu einer der Tabellenspalten oben als auch eine WHERE-Anweisung unter Verwendung des **Wohlbekannte Parameter** *(siehe 196)* `@ReportSessionId` beinhalten. Hierdurch wird sichergestellt, dass Sie die Daten für die aktuelle Ausführung des Berichts erhalten.

Beispiel

In den folgenden Beispielen wird der Kontext 'MachineFilter' verwendet.

```
SELECT COUNT(u.agentGuid) AS agentCount
FROM dbo.users u
INNER JOIN ReportCenter.MachineFilterList mfl ON mfl.AgentGuid = u.agentGuid
WHERE mfl.ReportSessionId = @ReportSessionid AND u.firstCheckin IS NOT NULL
```

So geben Sie ihn in das Dialogfeld zum Bearbeiten von Namenswert-Teilen ein:



Namenswert-Instanzen

Info Center > Konfiguration und Design > Namenswert-Teile

In einer **Namenswert-Instanz** werden die Argumente gespeichert, die den benutzerdefinierten **Parametern** *(siehe 194)* eines benutzerdefinierten Datasets zugewiesen wurden. Diese Namenswert-Instanzen können einem **Namenswert-Teil** *(siehe 189)* beigefügt werden, damit Argumente nicht jedes Mal, wenn eine Berichtsvorlage erstellt wird, manuell eingegeben werden müssen.

Felder

- **Name** – Der Name des benutzerdefinierten Datasets.
- **Wert-Label** – Die Beschriftung, die zusammen mit dem zurückgegebenen Wert des benutzerdefinierten Datasets angezeigt wird.

Parameter

Es handelt sich hierbei um die Argumente für jeden Parameter, die mit einer Instanz des benutzerdefinierten Datasets gespeichert sind.

Deckblatt-Kopf-/Fußzeile

Info Center > Konfiguration und Design > Deckblatt, Kopf- und Fußzeile

Auf der Seite **Deckblatt, Kopf-/Fußzeile** werden die Darstellungselemente definiert, die unabhängig von den im Bericht angezeigten Daten sind. Sie können mithilfe dieser Elemente Ihren Berichten ein einzigartiges Erscheinungsbild und eine persönliche Note verleihen. Weisen Sie einzelnen benutzerdefinierten Berichtsvorlagen und Berichtsdefinitionen unterschiedliche Kombinationen von Deckblättern, Kopf- und Fußzeilen zu.

Registerkarten

Jeder einzelne Elementtyp wird über eine separate Registerkarte definiert.

- **Deckblatt**
- **Kopfzeile**
- **Fußzeile**

Aktionen

Auf jeder Elementregisterkarte wird der gleiche Satz von Schaltflächen angezeigt.

- **Hinzufügen / Bearbeiten** – Zeigt das *Element-Designer-Fenster* an.
- **Löschen** – Löscht das Element.
- **Standard** – Legt dieses Element als Standard fest.
- **Vorschau** – Generiert eine Vorschau auf das Element.

Element-Designer-Fenster

Ziehen nach dem Öffnen des Element-Designer-Fensters eine beliebige Steuerung in eine der Zellen auf der rechten Seiten und legen Sie sie dort ab, um sie dem Seitenlayout des Elements hinzuzufügen. Danach werden in der Rasterzelle die folgenden Symbole angezeigt:

- – Hiermit wird das Rasterelement konfiguriert. Die hinzugefügten Steuerungen müssen zum Speichern des Elements konfiguriert werden.
- – Hiermit wird die Größe des Rasterelements geändert.
- – Hiermit wird das Rasterelement gelöscht.

Das Folgende wird in der Kopfzeile des Element-Designer-Fensters hinzugefügt oder geändert:

- **Name** – Der Name des Elements.

- **Beschreibung** – Die Beschreibung des Elements.
- **Standard** – Bei Aktivierung dient dieses Element beim Erstellen einer Berichtsvorlage als Standard.

Deckblattsteuerung

Die folgenden Steuerungen stehen im Element-Designer-Fenster für die Elemente auf dem **Deckblatt** zur Verfügung.

- **Berichts-Logo** – Legt die Breite, Höhe und die Ausrichtung des Berichts-Logos fest.

  Hinweis: Standardmäßig zeigen VSA-Berichtskopfzeilen das unter "System > Seitenanpassung > **Website-Kopfzeile** *(siehe 448)*" angegebene Bild an. Durch Änderung des Werts in "System > Konfigurieren > **Berichtskonfiguration ändern** *(siehe 434)* > **Logo**" können Sie diese Standardeinstellung überschreiben und die URL *nur für Berichtskopfzeilen ändern*. Die Änderung der URL im Feld "Berichtskonfiguration ändern > **Logo**" wirkt sich nicht auf das Bild in der **Website-Kopfzeile** aus.

- **Textfeld** – Gibt den Text, die Ausrichtung und das Format eines Textfeldes an. Die Steuerungen **Textfeld** und **Textbereich** unterstützen beide die folgenden eingebetteten Tags.
  `<rt>` = Berichtsname
  `<rd>` = Berichtsdatum
  `<org>` = Organisationsfilter
  `<gr>` = Rechnergruppenfilter
  `<id>` = Rechnerfilter
- **Textbereich** – Gibt den Text, die Ausrichtung und das Format eines Textbereiches an.
- **Filtertabelle** – Beinhaltet eine Legende mit einer Beschreibung der auf den Bericht angewendeten Filterung.
- **Horizontale Linie** – Gibt das Format und die Farbe einer horizontalen Linie an, die andere Zeilen im Raster voneinander trennt.
- **Abstandszeichen** – Gibt die Größe des vertikalen Leerraums zwischen den Zeilen im Raster an.

Kopf- und Fußzeilen-Steuerungen

Die folgenden Steuerungen stehen im Element-Designer-Fenster für die Elemente der **Kopfzeile** und der **Fußzeile** zur Verfügung.

- **Textfeld** – Gibt den Text, die Ausrichtung und das Format eines Textfeldes an.
- **Seiten-Nr.** – Gibt den Text, die Ausrichtung und das Format einer Seitennummer an.

Standardeinstellungen

Info Center > Konfiguration und Design > Standardeinstellungen

Auf der Seite **Standardeinstellungen** werden die Einstellungen festgelegt, die für Berichtsdefinitionen standardmäßig gelten sollen. Zu den Standardeinstellungen gehören:

- **Standard-Papiergröße**
- **Standard-Verteilung**

Alte Berichtsdefinitionen

Ein Bericht wird basierend auf einer Berichtsdefinition veröffentlicht. Berichtsdefinitionen enthalten alle *Standard*einstellungen, mit denen Inhalt, Layout und Dateiformat eines veröffentlichten Berichts festgelegt werden. Sie können beim Ausführen (Veröffentlichen) oder Planen des Berichts diese Standardeinstellungen überschreiben.

Beim Erstellen einer Berichtsdefinition werden Berichtsdefinitionseinstellungen aus einer Berichtsvorlage kopiert. Durch das Ändern einer Berichtsdefinition wird nicht die Berichtsvorlage, aus der sie kopiert wurde, geändert. An einer Berichtsvorlage vorgenommene Änderungen haben keine Auswirkungen auf die Berichtsdefinitionen, die bereits aus dieser Vorlage kopiert wurden.

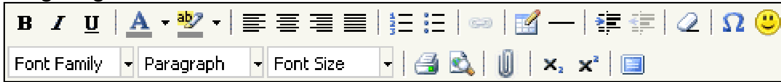
So erstellen Sie eine *alte Berichtsdefinition* basierend auf einer *Berichtsvorlage*:

1. Klicken Sie auf **Info Center > Reporting > Berichte > Neu**.
2. Wählen Sie die Option **Alter Bericht**.
3. Wählen Sie eine **Kategorie**, dann eine **Vorlage** und klicken Sie anschließend auf **Erstellen**.
4. Geben Sie unter Verwendung der Kopfzeilenoptionen und dreier Registerkarten Optionen für Berichtsdefinitionen an:
   - **(Kopfzeilenoptionen)** – Geben Sie den Namen und Titel des Berichts an. Außerdem können Sie festlegen, dass **für den Bericht eine Genehmigung erforderlich** *(siehe 171)* ist.
   - **Parameter** – Eine Beschreibung dieser Parameter finden Sie in der Liste der vordefinierten *alten Berichtsvorlagen* unten.

   > **Hinweis:** Beim Hinzufügen oder Bearbeiten einer *benutzerdefinierten* **Berichtsdefinition** *(siehe 165)* wird die Registerkarte **Layout** statt der Registerkarte **Parameter** angezeigt.

   - **Allgemein** – Bestimmt die Art der Ausgabe – PDF, HTML oder EXCEL –, Papiergröße und Ausrichtung. Mit dieser Option wird außerdem die Nachricht festgelegt, mit der Benutzer über den Zeitpunkt der Ausführung des Berichts benachrichtigt werden. Tokens können in E-Mail-Nachrichten für Berichte – sowohl in der Betreffzeile als auch im Nachrichtentext – mit aufgenommen werden.
     - ✓ `<gr>` – Rechnergruppe
     - ✓ `<id>` – Rechner-ID
     - ✓ `<rt>` – Berichtsname
     - ✓ `<embd>` – Sie können nur im Nachrichtentext einen HTML-Bericht an der angegebenen Stelle einbetten.

     Über die Werkzeugleiste zum Bearbeiten können Sie Bilder und eine besondere Formatierung zum Text hinzufügen. Bilder müssen hochgeladen anstatt kopiert und eingefügt werden.

     - ✓ – Hyperlink für ausgewählten Text. Möglicherweise müssen Sie Links, die von einer anderen Quelle eingefügt wurden, zurücksetzen.
     - ✓ – Tabelle einfügen
     - ✓ – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
     - ✓ – Text einrücken
     - ✓ – Text ausrücken
     - ✓ – Formatierung entfernen
     - ✓ Ω – Symbol einfügen
     - ✓ – Emoticon einfügen

- ✓ – Bild- und Textvorschau anzeigen
- ✓ – Datei oder Bild hochladen
- ✓ – Ausgewählten Text tiefgestellt festlegen
- ✓ – Ausgewählten Text hochgestellt festlegen
- ✓ – Vollbildmodus zur Ansicht und Bearbeitung ein- und ausschalten

➢ **Deckblatt, Kopf- und Fußzeile** – Hierdurch werden **Deckblatt, Kopf- und Fußzeile** *(siehe 201)* des Berichts ausgewählt

Sie können alte Berichtsdefinitionen basierend auf den folgenden alten Berichtsvorlagen erstellen.

In diesem Abschnitt

Antivirus-Installations-Statistik

Info Center > Reporting > Berichte > Antivirus

- *Wird nur angezeigt, wenn das Antivirus-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Antivirus-Installations-Statistik** werden Berichte für die folgenden Arten von **Antivirus**-Daten generiert, die vom VSA gepflegt werden.

- **Übersichtstabelle anzeigen** – Zeigt die Anzahl der Rechner an, die pro Rechnergruppe bei **Antivirus** installiert sind. Installationsdetails umfassen das Installationsdatum und die installierte Version pro Rechner in jeder Rechnergruppe.
- **Installationsmonat-Balkendiagramm anzeigen** – Zeigt die Anzahl der mit **Antivirus** installierten Rechner pro Monat an.

Antischadsoftware – Antischadsoftware-Installationsstatistik

Info Center > Reporting > Berichte > Antischadsoftware

- *Wird nur angezeigt, wenn das AntiMalware-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Antischadsoftware-Installationsstatistik** werden Berichte für die folgenden Arten von **AntiMalware**-Daten generiert, die vom VSA gepflegt werden.

- **Übersichtstabelle anzeigen** – Zeigt die Anzahl der Rechner an, die pro Rechnergruppe bei **AntiMalware** installiert sind. Installationsdetails umfassen das Installationsdatum und die installierte Version pro Rechner in jeder Rechnergruppe.
- **Installationsmonat-Balkendiagramm anzeigen** – Zeigt die Anzahl der mit **AntiMalware** installierten Rechner pro Monat an.

Inventarisierung – Aggregattabelle

Info Center > Reporting > Berichte > Audit - Aggregattabelle

Mit der Berichtsdefinition **Aggregattabelle** wird ein tabellarischer Bericht generiert, in den alle vom VSA erfassten Daten aufgenommen werden. Jeder Bericht generiert eine einzelne Tabelle mit einer Zeile für jeden Rechner und einer Spalte für jedes angegebene Datenelement.

Elemente hinzufügen oder entfernen

Zum Hinzufügen von Elementen, wählen Sie die gewünschten Elemente auf der linken Seite aus und klicken dann mit der rechten Pfeiltaste. Zum Entfernen von Elementen, wählen Sie die gewünschten Elemente auf der rechten Seite aus und klicken dann mit der linken Pfeiltaste. Zum Ändern der Reihenfolge der aufgelisteten Elemente klicken Sie auf ein Element in der rechten Liste und klicken dann auf die Pfeiltaste nach oben oder unten.

Erweiterter Filter

Klicken Sie auf die Registerkarte **Erweiterter Filter** *(siehe 30)*, um die angezeigte Datenmenge einzuschränken. Sie können für jede Spalte der angezeigten Daten einen anderen erweiterten Filter angeben.

Inventarisierung – Plattennutzung

Info Center > Reporting > Berichte > Audit - Plattennutzung

Mit der Berichtsdefinition **Plattennutzung** wird ein grafischer Bericht generiert, in dem der freie und der belegte Speicherplatz sowie der Speicherplatz insgesamt auf jedem Laufwerk dargestellt wird.

Es sind drei Arten von Berichten verfügbar:

- **Balkendiagramm mit genutztem Plattenspeicherplatz anzeigen**
- **Balkendiagramm mit genutztem Plattenspeicherplatz, freiem Speicherplatz und Plattenkapazität anzeigen**
- **Tabelle mit genutztem Plattenspeicherplatz, freiem Speicherplatz und Plattenkapazität anzeigen**

Inventarisierung – Bestand

Info Center > Reporting > Berichte > Audit - Inventarisierung

- Ähnliche Informationen werden über Audit > Systeminformationen *(siehe 154)* bereitgestellt.

Mit der Berichtsdefinition **Bestand** wird ein Bericht generiert, in dem alle während einer Inventarisierung erfassten Elemente eindeutigen Elemente aufgelistet werden. Außerdem werden die Rechner angegebenen, die dieses Element enthalten.

Filtern

Filter schränken die in dem Inventarisierungsbericht aufgeführten Elemente auf solche ein, die dem Filter entsprechen. Wenn Sie beispielsweise einen Bestandsbericht für das Feld **Motherboardhersteller** ausführen und den Filter auf `*Intel*` setzen, so werden in dem Bericht nur Elemente aufgelistet, die von `Intel` oder `Intel Corp` oder einer anderen Variation dieses Herstellernamens hergestellt wurden.

PCI & Disk-HW-Bestandsberichte

Mit der Option `PCI & Disk-HW` werden weitere Felder angezeigt, nach denen Sie die Daten im Bericht filtern können.

- **Hardwaretyp**
- **Beschreibungs-/Anmerkungsfilter**
- **Produktfilter**
- **Lieferantenfilter**

Inventarisierung – Änderungen an Rechnern

Info Center > Reporting > Berichte > Audit - Änderungen an Rechnern

- Ähnliche Informationen werden über Audit > Systeminformationen *(siehe 139)* sowie Installierte Anwendungen *(siehe 156)* bereitgestellt.

Mit der Berichtsdefinition **Änderungen an Rechnern** wird eine Aufstellung der Unterschiede zwischen der letzten Inventarisierung des Rechners und der rechnereigenen Referenzinventarisierung *oder* ein Vergleich zwischen der Referenzinventarisierung bzw. der letzen Inventarisierung und einem ausgewählten Rechner generiert. Die geprüften Änderungen an Rechnern umfassen CPU, RAM, Plattenspeicher und installierte Anwendungen.

Konfigurieren Sie Ihren Bericht unter Verwendung der folgenden Optionen:

- **Mit der rechnereigenen Referenzinventarisierung vergleichen** – Zeigt alle Änderungen an, die auf allen Rechnern gefunden wurden, indem die Informationen der letzten Inventarisierung mit den Informationen der Referenzinventarisierung verglichen werden.
- **Mit ausgewählter Rechner-ID vergleichen** – Zeigt alle Änderungen an, die auf allen Rechnern gefunden wurden, indem die Informationen der letzten Inventarisierung mit den Informationen der Inventarisierung einer *ausgewählten Rechner-ID* verglichen werden. Anhand dieser Funktion können Sie Unterschiede in einer Gruppe von Rechnern im Vergleich zu den Standardangaben für die Gruppe identifizieren.
- **Referenzinventarisierung verwenden** – Aktiviert, wenn **Mit ausgewählter Rechner-ID vergleichen** ausgewählt ist. Wenn diese Option aktiviert ist, wird die Referenzinventarisierung der Rechner-ID anstelle der letzten Inventarisierung der Rechner-ID für den Vergleich verwendet.

Inventarisierung – Rechnerübersicht

Info Center > Reporting > Berichte > Audit - Rechnerübersicht

- Über Audit > Rechnerübersicht *(siehe 151)* und Live-Connect *(siehe 393)* werden ähnliche Informationen bereitgestellt.

Die Berichtsdefinition **Rechnerübersicht** generiert einen detaillierten Bericht für jede Rechner-ID, die mit dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 626)* übereinstimmt. Mit dem Bericht **Rechnerübersicht** können Sie ausführliche Berichte zu einzelnen Rechnern generieren. Es werden separate Hinzufügen/Entfernen-Auswahlfenster für System- und Anwendungsdaten bereitgestellt, die in den Bericht **Rechnerübersicht** eingeschlossen werden sollen.

Abschnitte der Rechnerübersicht

Der Bericht **Rechnerübersicht** kann die folgenden Abschnitte enthalten:

- **Programme hinzufügen/entfernen** – Listet Programme in der Hinzufügen/Entfernen-Liste eines verwalteten Rechners auf.
- **Agent-Kontrolle/Check-In** – Zeigt Informationen zur Anfangsprüfung und aktuellen Inventarisierungen, den letzten Check-in-Zeiten, Kurz-Check-in-Perioden, dem primären und sekundären Server und Portinformationen an.
- **Anwendungen** – Listet die auf dem verwalteten Rechner installierten Anwendungen auf. Die Liste der Anwendungen kann durch Klicken auf die Schaltfläche **Anwendungsfilter** gefiltert werden.
- **Seit Referenzinventarisierung hinzugefügte Anwendungen** – Alle durch **Letzte Inventarisierung** *(siehe 146)* ermittelten neuen Anwendungen, die seit der **Referenzinventarisierung** *(siehe 146)* auf dem Rechner hinzugefügt wurden.
- **Seit Referenzinventarisierung entfernte Anwendungen** – Alle Anwendungen, die bei der **Referenzinventarisierung** *(siehe 146)* vorlagen, jedoch beim Ausführen der **Letzten Inventarisierung** *(siehe 146)* fehlten.
- **Computer/Netzwerk** – Zeigt Windows-Netzwerknamen, Betriebssystem, CPU, RAM, IP-Adresse, Gateway, DNS/DHCP-Server, und WINS-Serverinformationen des verwalteten Rechners an.
- **Dateien verteilen** – Listet die Dateien auf, die vom Kaseya Server an den verwalteten Rechner verteilt werden.

- **Dateizugriff** – Listet geschützte Dateien auf.
- **Lizenzcodes** – Listet die auf dem verwalteten Rechner installierten Lizenzcodes auf.
- **Logische Festplatte** – Listet die logischen Datenträger auf den verwalteten Rechnern auf, einschließlich fest eingebauten, CD-ROM- und Wechsellaufwerken.
- **Verschiedenes** – Listet verschiedene Agent-Einstellungen auf, wie beispielsweise WinVNC und Benutzerprotokollstatus.
- **Netzwerkzugriff** – Listet Anwendungen mit beschränktem Netzwerkzugriff auf.
- **PCI-Geräte** – Listet die auf dem verwalteten Rechner installierten PCI-Geräte auf.
- **Anstehende Verfahren** – Listet die geplanten Verfahren auf dem verwalteten Rechner auf.
- **Physikalische Festplatte** – Listet Informationen zu den physikalischen Festplatten des verwalteten Rechners auf, wie beispielsweise Festplatten, DVD- und CD-ROM-Laufwerke.
- **Drucker** – Listet die bei der Inventarisierung für diesen Rechner gefundenen Drucker auf.
- **Periodische Verfahren** – Listet Verfahren auf, die regelmäßig auf dem verwalteten Rechner ausgeführt werden.
- **Systeminformationen** – Alle durch die Funktion **Systeminformationen** *(siehe 154)* im **Inventarisierung**smodul erfassten Elemente. Klicken Sie auf die Schaltfläche **Systeminfo**, um weitere Systeminformationen auszuwählen.
- **Benutzerprofil** – Listet Benutzerkontaktinformationen zu dieser Rechner-ID auf.

Elemente hinzufügen oder entfernen

Zum Hinzufügen von Elementen, wählen Sie die gewünschten Elemente auf der linken Seite aus und klicken dann mit der rechten Pfeiltaste. Zum Entfernen von Elementen, wählen Sie die gewünschten Elemente auf der rechten Seite aus und klicken dann mit der linken Pfeiltaste. Zum Ändern der Reihenfolge der aufgelisteten Elemente klicken Sie auf ein Element in der rechten Liste und klicken dann auf die Pfeiltaste nach oben oder unten.

Erweiterter Filter

Klicken Sie auf die Registerkarte **Erweiterter Filter** *(siehe 30)*, um die angezeigte Datenmenge einzuschränken. Sie können für jede Spalte der angezeigten Daten einen anderen erweiterten Filter angeben. Diese Option wird nur angezeigt, wenn die Option **Systeminformationen** weiter oben aktiviert wurde.

Inventarisierung – Netzwerkstatistik

Info Center > Reporting > Berichte > Netzwerkstatistik

- Über Info Center > Reporting > Berichte > Protokolle > Netzmaske-Statistik-Protokoll *(siehe 221)* werden *alle* Netzwerkzugriffsaktivitäten identifiziert.
- Zugehörige Informationen werden über System > Statistiken *(siehe 442)* bereitgestellt.

Mit der Berichtsdefinition **Netzwerkstatistik** wird ein Bericht generiert, in dem die *Hauptverbraucher* der auf dem TCP/IP-Protokoll basierten Netzwerkbandbreite auf ausgewählten Rechnern angezeigt werden. Dieser Bericht bezieht sich in der Regel auf den Bandbreitenverbrauch durch den Zugriff auf interne und externe *Internet*-Sites. Er kann jedoch auch internen LAN-Verkehr, der das TCP/IP-Protokoll verwendet, einschließen

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Berichtsparameter

- **Anwendungen** – Zeigt ein Diagramm an, das einen Überblick über die einzelnen Anwendungen und ihren jeweiligen Netzwerkbandbreitenverbrauch über den angegebenen Zeitraum gibt.
- **Rechner** – Zeigt ein Diagramm an, das einen Überblick über die im Rechner-ID-/Gruppen-ID-Filter ausgewählten Rechner und ihren entsprechenden Netzwerkbandbreitenverbrauch gibt.
- **Führende <N> Bandbreitenverbraucher anzeigen** – Die Anzahl der Hauptverbraucher von Bandbreite, die in den Bericht aufgenommen werden. Dies können Anwendungen oder Rechner sein.

> **Hinweis:** Für dieses Protokoll muss der Treiber Audit > **Netzwerkzugriff** *(siehe 84)* aktiviert sein. Dieser Treiber fügt sich in den TCP/IP-Stapel ein, um den auf dem TCP/IP-Protokoll basierenden Datenverkehr nach Anwendung zu messen. Er ist standardmäßig *deaktiviert*.

Backup – Backup

Info Center > Reporting > Berichte > Backup

- Wird nur angezeigt, wenn das Sicherungs-Zusatzmodul installiert ist.
- Über Backup > Backup-Status werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Sicherung** wird ein Bericht generiert, in dem die von den Sicherungsprotokollen abgerufenen Daten zusammengefasst werden.

Konfigurieren Sie Ihren Bericht unter Verwendung der folgenden Optionen:

- **Backup-Protokolle zeigen der letzten N> Tage** – Geben Sie an, wie viele Tage mit Backup-Protokolleinträgen in den Bericht aufgenommen werden sollen.
- **Sicherungsprotokoll-Übersichtdaten anzeigen** – Wenn diese Option aktiviert ist, wird eine Übersichtstabelle der Sicherungsereignisse der letzen N Tage für Datenträger und Ordner eingeschlossen.
- **Sicherungsprotokollstatus pro Rechner und Vorgang anzeigen** – Führt die Sicherungsprotokollinformationen der letzten N Tage für jeden Rechner auf.
  - **Filter für Backuptyp** – `Volume-Backups` oder `Ordner-Backups`.
  - **Ergebnisfilter** – `<Alle Ergebnisse<, Erfolg, Versagen, Warnung, Zur Information`
- **Rechner ohne Daten ignorieren** – Wenn diese Option aktiviert ist, wenn nur Rechner-IDs mit Daten angezeigt, die den anderen Filterparametern entsprechen.

Desktop Management – Energieeinsparungen

Info Center > Reporting > Berichte > Desktop Management > Energieeinsparungen

- Wird nur angezeigt, wenn das Desktop Policy-Zusatzmodul installiert ist.

Auf der Seite **Energieeinsparungen** generieren Sie einen Bericht, in dem Sie ablesen können, wie viel Geld Sie mit einer bestimmten Energieregel schätzungsweise sparen können bzw. bereits gespart haben. Eine unabhängige Energieprüfung wird im Rahmen der Standardprüfung geplant. Diese erfasst Energieeinstellungen von allen verwalteten Rechnern, *einschließlich solchen, bei denen der* **Desktop Policy**-*Client nicht installiert ist*.

Vergleichseinstellungen

Eine Energieprüfung wird immer dann auf einem Rechner ausgeführt, wenn eine Energieregel auf den Rechner angewendet wird. Sie wird auch bei der **letzten Inventarisierung** *(siehe 615)* (meist täglich) ausgeführt.

- **Vergleichen Sie die Basis-Audit-Daten des Rechners mit:**

- **Vergleichen mit** – Wählen Sie eine definierte Energieregel aus, um zu sehen, wie viel Geld Sie bei der Umstellung auf die ausgewählte Energieregel sparen könnten.
- **Alle Rechner miteinbeziehen** – Wenn diese Option aktiviert ist, werden die unabhängigen Energieprüfungsergebnisse für alle Windows 2003- und Windows XP-Rechner ohne **Desktop Policy** zusammen mit den Ergebnissen für Rechner, auf denen **Desktop Policy** installiert ist, miteinbezogen. Diese Option ist standardmäßig aktiviert. Windows 2000-, Vista- und 7-Rechner werden nicht eingeschlossen.

- **Vergleichen Sie die aktuellsten Energie-Audit-Daten mit:**
  - **Vergleichen mit** – `Basis-Energie-Richtlinie` – Zeigt die Energieersparnisse an, indem die Basis-Energie-Richtlinie mit dem aktuellen Überprüfungsergebnis für jeden Rechner verglichen wird. Die Basis-Energie-Richtlinie stellt den Zustand vor der Installation von **Desktop Policy** auf dem Rechner dar.
  - **Vergleichen mit** – `Letzte bereitgestellte Energie-Richtlinie` – Zeigt die Energieersparnisse an, indem die letzte bereitgestellte Energie-Richtlinie mit dem aktuellen Überprüfungsergebnis für jeden Rechner verglichen wird. Dieser Wert sollte mit den Daten der letzten Energieprüfung identisch sein, es sei denn, irgendwelche Benutzer haben seit der letzten Anwendung einer Energieregel ihre Einstellungen geändert.
- **Berichtsperiode** – Geben Sie die Berichtsperiode für den Bericht ein: `Year`, `Month`, `From Baseline Collection Time`.

Berichtswerte einstellen

Bestimmen Sie die Werte, auf denen die Schätzwerte für die Energieersparnisse basieren, oder belassen Sie sie bei den Standardwerten.

- **Durchschnittliche PC-Watt** – Geben Sie die Anzahl der Watt ein, die ein durchschnittlicher PC im System verbraucht.
- **Durchschnittliche Monitor-Watt** – Geben Sie die Anzahl der Watt ein, die ein durchschnittlicher Monitor im System verbraucht.
- **Kosten pro Kilowattstunde (kWh)** – Geben Sie die Kosten pro Kilowattstunde (kWh) ein.
- **Währungssymbol** – Geben Sie das Währungssymbol für die in das Feld **Kosten pro Kilowattstunde** eingegebenen Kosten ein. Das Währungssymbol wird in dem Bericht angezeigt.

Erweiterte Einstellungen

Nehmen Sie Änderungen an den folgenden erweiterten Einstellungen vor oder belassen Sie sie auf ihren Standardwerten:

- **PC-Watt in Standby** – Geben Sie die Anzahl der Watt ein, die ein durchschnittlicher PC im Standby-Modus verbraucht.
- **Workstation-Stunden pro Tag** – Geben Sie die Anzahl der Stunden ein, die eine Workstation pro Tag in Verwendung ist.
- **Workstation-Stunden pro Woche** – Geben Sie die Anzahl der Stunden ein, die eine Workstation pro Woche in Verwendung ist.
- **% der abgeschalteten Rechner am Ende des Tages** – Geben Sie die Anzahl der Rechner ein, die am Ende des Tags ausgeschaltet werden.
- **Workstation Leerlauftage pro Jahr (Feiertage, Urlaube usw.)** – Geben Sie die Anzahl der Tage pro Jahr ein, die eine Workstation normalerweise nicht in Verwendung ist (zusätzlich zu Wochenenden).
- **Auswahl der Rechnerdaten auf Basis von:**
  - **Die meisten Einsparungen** – Wenn diese Option aktiviert ist, verwendet die Berechnung einen einzelnen Benutzer auf einem Rechner, der die höchsten geschätzten Einsparungen erzielt, selbst wenn kein anderer Benutzer jemals diesen Rechner verwendet hat. Dies stellt die bestmöglichen Energieersparnisse für diesen Rechner dar.
  - **Durchschnittlicher Benutzer** – Wenn diese Option aktiviert ist, verwendet die Berechnung einen Durchschnitt der geschätzten Energieersparnisse aller Benutzer auf einem Rechner, als ob

jeder Benutzer für den gleichen Zeitraum bei diesem Rechner angemeldet wäre. Damit erhalten Sie einen gleichwertigen oder niedrigeren Energieersparnis-Schätzwert als mit der Option **Die meisten Einsparungen**.

- **Festplatten-Watt** – Geben Sie die Anzahl der Watt ein, die eine Festplatte verbraucht.
- **Server-Stunden pro Tag** – Geben Sie die Anzahl der Stunden ein, die ein Server pro Tag in Verwendung ist.

> **Hinweis:** Jedes Betriebssystem, dessen Name das Wort Server enthält, wird im Rahmen dieses Berichts als Server behandelt.

- **Server-Tage pro Woche** – Geben Sie die Anzahl der Tage ein, die ein Server pro Woche in Verwendung ist.
- **Monitore für Server einschließen** – Wenn diese Option aktiviert ist, wird bei der Berechnung davon ausgegangen, dass an den Server ein Monitor angeschlossen ist und dass die Energieeinstellungen für die Monitore eingeschlossen werden.
- **Einstellungen pro Benutzer anzeigen** – Wenn diese Option aktiviert ist, werden in dem Bericht die Einsparungen für jeden Benutzer auf jedem Rechner angezeigt.

Desktop Management – Benutzerstatus

Info Center > Reporting > Reports > Desktop Management > Benutzerstatus

- Wird nur angezeigt, wenn das Desktop Policy-Zusatzmodul installiert ist.
- Ähnliche Informationen werden über Desktop Management > Status bereitgestellt.

Auf der Seite **Desktoprichtlinie** werden Berichte für die folgenden Arten von **Desktop Policy**-Daten generiert, die vom VSA gepflegt werden.

Wählen Sie die Unterthemen aus, die in den **Desktop Policy**-Bericht mit aufgenommen werden sollen:

- **Benutzertyp einschließen** – Hier werden alle Benutzergruppen aufgeführt, bei denen jeder Benutzer des Rechners ein Mitglied ist.
- **Zugeordnete Laufwerke einschließen** – Listet die Laufwerkszuordnungen für jeden Benutzer auf.
- **Drucker einschließen** – Listet die Druckerzuordnungen für jeden Benutzer aus.
- **Sharepoints einschließen** – Listet alle Verzeichnisfreigaben für den Rechner auf.
- **Rechner ohne Daten miteinbeziehen** – Zeigt Einträge für alle Rechner in dem Bericht an, einschließlich derjenigen, für die keine **Desktop Policy**-Informationen erfasst wurden.

Executive – Executive-Übersicht

Info Center > Reporting > Berichte > Executive - Executive Summary

Mit der Berichtsdefinition **Executive-Übersicht** wird ein Übersichtsbericht des Status aller ausgewählten Rechner generiert. Dies schließt eine **Netzwerkleistungsbewertung** *(siehe 213)* ein, die Systemzustand aller ausgewählten Rechner als Gruppe darstellt.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Daten zusammenfassen, die in den letzten N Tagen erfasst wurden** – Anzahl der Tage, rückwirkend seit dem aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen

Berichtsparameter – Berichtsauswahl

- **Clientinformationen zeigen** – Zeigt die Anzahl der Rechner (inkl. Server und Workstations) sowie die Namen der primären Kontaktpunkte für diese Gruppe an.
  - **Kontaktperson** – Geben Sie wahlweise einen Kundenkontaktnamen ein, der den Kontaktpunkt innerhalb der Organisation, die diesen IT-Dienst erhält, darstellt.

- **IT-Manager** – Geben Sie wahlweise den Namen eines IT-Managers ein, der als Verantwortlicher für die Zustellung der IT-Dienste an die Clientorganisation fungiert.

- **Systemaktivität zeigen** – Geben Sie Suchkriterien an, um zu ermitteln, wie oft bestimmte Protokollereignisse eingetreten sind. Beispiele hierfür sind die Angabe, wie oft Rechner kontrolliert und auf fehlende Patches gescannt wurden. Klicken Sie auf **Zeilen ändern...**, um diesen Abschnitt anzupassen.
- **Ticketstatus zeigen** – Zeigt eine Übersicht über die Ticketzahlen während der angegebenen Anzahl von Tagen an. Wenn **Service Desk** installiert und aktiviert ist, wird die Ticketanzahl nur für **Service Desk**-Tickets angezeigt. Weitere Ticketzahlen für die Anzahl der Tickets in jedem definierten `Status` werden angezeigt. `Nicht kategorisierte Tickets` wird angezeigt, wenn für ein oder mehrere Tickets kein `Status` angegeben wurde.
- **Antivirus-Statistik anzeigen** – Zeigt die **Statistiken** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#7189.htm)* zum Antivirusschutz und den Bedrohungen an.

  > **Hinweis:** Der Abschnitt **Antivirus-Statistik anzeigen** wird nur angezeigt, wenn Sie das Antivirus-Zusatzmodul installiert haben.

- **Verwendeten Plattenspeicherplatz anzeigen für** – Zeigt ein Diagramm des prozentualen Anteils von freiem Speicherplatz auf allen ausgewählten Rechnern an. Sie können dieses Diagramm auf Server einschränken, indem Sie die Option `Nur Server zeigen` aktivieren.
- **Prozent der Laufzeit anzeigen für** – Zeigt ein Diagramm des prozentualen Anteils der Rechner an, die gegenwärtig ausgeführt werden. Sie können dieses Diagramm auf Server einschränken, indem Sie die Option `Nur Server zeigen` aktivieren.
- **Netzwerk-Leistungsauswertung zeigen** – Zeigt den Systemzustand einzelner Komponenten und den Systemzustand aller ausgewählten Rechner in einer Gruppe insgesamt an. Weitere Informationen finden Sie unter **Netzwerk-Leistungsauswertung** *(siehe 213)*. Klicken Sie auf **Bewertung ändern...**, um diesen Abschnitt anzupassen.
- **Betriebssysteme zeigen** – Zeigt ein Kreisdiagramm des prozentualen Anteils der verschiedenen Betriebssysteme in der ausgewählten Gruppe an.
- **Patch-Status zeigen** – Zeigt ein Kreisdiagramm an, das einen Überblick über den Status der fehlenden Patches für alle ausgewählten Rechner bietet.
- **Sicherheit zeigen** – Führt Statistiken zu nicht behobenen Bedrohungen des Sicherheitsschutzes an.

  > **Hinweis:** Der Abschnitt **Sicherheit anzeigen** wird nur angezeigt, wenn Sie das Endpoint Security-Zusatzmodul installiert haben.

- **Alarmmeldungen anzeigen** – Hier erhalten Sie eine Übersicht über die Alarme, die in der angegebenen Anzahl von Tagen ausgegeben wurden. Die Anzahl der Alarme wird nach Kategorie aufgeschlüsselt.
- **Überblick über Lizenzen zeigen** – Bietet einen Überblick über die in einem Audit gefundenen Betriebssystem- und MS Office-Lizenzen.
- **Weiterführende Anmerkungen am Ende des Berichts anzeigen** – Zeigt erläuternde Anmerkungen am Ende des Berichts an. Klicken Sie auf **Anmerkungen bearbeiten...**, um diese Anmerkungen anzupassen.

Systemaktivität

Info Center > Reporting > Berichte > Executive Summary > Systemaktivität

Im Abschnitt **Systemabläufe** des Berichts **Executive-Übersicht** *(siehe 211)* finden Sie einen Überblick über die Systemabläufe der ausgewählten Rechner als eine Gruppe. Auf jeder Zeile wird eine *Zahl* oder ein *Wert* eines gefilterten Protokollelements in den *letzten N Tagen* aufgelistet.

- Anhand der Spalte **Status** auf der Registerkarte **Anstehende Verfahren** der Seite **Rechnerübersicht** *(siehe 207)* oder **Live Connect** *(siehe 393)* können Sie Suchfilterausdrücke identifizieren, die für einen verfahrensbasierten Zeilentyp verwendet werden sollen.

  > **Hinweis:** Sie müssen mindestens ein * in das Feld **Suchfilter** eingeben, um Ergebnisse zu erhalten.

- **Protokoll-Monitoring** wird nicht in **Anstehende Verfahren** angezeigt. Prüfen Sie **Protokoll-Monitoring** in **Agent-Protokolle** auf der Seite **Rechnerübersicht** oder **Live Connect**, um die zu verwendenden Suchfilterausdrücke zu identifizieren.
- **Protokoll-Monitoring benutzerdefiniert** bezieht sich auf den *Wert oder die Zahl* eines Analyseparameters für ein numerisches Protokoll innerhalb der *letzten N Tage*.

Zeilentyp	Element suchen	Suchfilterbeispiele	Anzahl
Alarmprotokoll	`<Alle Alarme>` oder ein(e) bestimmte(r) Meldung bzw. Alarm	`* or *text*`	Nicht zutreffend
Skriptprotokoll	Wählen Sie ein System-, ein privates oder ein öffentliches Agent-Verfahren aus.	`*Success THEN*` oder `*Failed ELSE*` oder `*Success ELSE*`	Nicht zutreffend
Backup-Protokoll	`<All Backup Events>` oder `Volume Backups` oder `Folder Backups`	`*Backup completed successfully*`	Nicht zutreffend
Protokoll-Monitoring	Wählen Sie eine **Protokolldateianalyse** *(siehe 359)* aus.	`*device error*`	Nicht zutreffend
Protokoll-Monitoring benutzerdefiniert	Wählen Sie eine Protokolldateianalyse mit einem numerischen Parameter aus.	`EventCode` oder `ErrorCode`	`Durchschnitt`, `Anzahl`, `Min`, `Max` oder `Gesamt`

Netzwerkstatus-Auswertung

Info Center > Reporting > Berichte > Executive Summary > Bewertung ändern...

Im Abschnitt **Netzwerk-Leistungsauswertung** des Berichts **Executive-Übersicht** *(siehe 211)* finden Sie einen Überblick über den Zustand und Nutzbarkeit der ausgewählten Rechner als eine Gruppe. Die Bewertung ist in die folgenden **Bewertungstypen** aufgeschlüsselt. Jeder Bewertungstyp ist in einen von fünf möglichen **Prozent-Buckets** unterteilt, in der Regel 100%, 75%, 50%, 25% und 0%, falls keiner der ersten vier Prozent-Buckets anwendbar ist, basierend auf der Zählung nach bestimmten Kriterien.

Beispiel für die Berechnung des Bewertungstyps: Ein einfacher **Executive-Übersicht**sbericht enthält lediglich drei Rechner. Für einen einzelnen Bewertungstyp innerhalb dieses Berichts muss ein Rechner die Kriterien für den 100%-Bucket erfüllen. Die beiden anderen Rechner erfüllen die Kriterien für den 75%-Bucket. (100% + 75% + 75%)/3 = 83% Systemzustand für diesen Bewertungstyp. Sie können einen Stellenwert von 2 zuweisen, um den Stellenwert dieses Bewertungstyps im Vergleich zu allen anderen Bewertungstypen in dem Bericht zu verdoppeln.

Beispiel für die Berechnung des Stellenwerts: Sie stellen einen Bewertungstyp auf einen Stellenwert von 2 und sieben Bewertungstypen auf einen Stellenwert von 1 ein. Der Gesamtstellenwert aller *8* Bewertungstypen ist *9*. Der Prozentsatz des Bewertungstyps mit dem Stellenwert 2 wird für die Berechnung der endgültigen prozentualen Bewertung mit 2/9 multipliziert. Im Gegensatz hierzu werden die Prozentsätze der anderen sieben Bewertungstypen mit dem Stellenwert 1 zur Berechnung der endgültigen prozentualen Bewertung mit 1/9 multipliziert.

Die endgültige Netzwerkleistungsbewertung ergibt sich aus dem *gewichteten Durchschnitt* der

Prozentsätze aller Bewertungstypen. Dieser wird für die Berechnung der endgültigen prozentualen Bewertung normalisiert. 100% stellt einen perfekten Zustand dar.

- In den meisten Fällen können Sie die Angaben anpassen, die zur Zuweisung prozentualer Bewertungen verwendet werden.
- Setzen Sie den Stellenwert auf *0, um diesen Bewertungstyp zu deaktivieren*.
- Für den **Betriebssystembewertung**styp werden die standardmäßigen prozentualen Buckets von 100%, 75%, 50% und 25% durch die von Ihnen festgelegten Werte überschrieben. Jeder Bucket ist einem anderen Betriebssystemtyp verknüpft. Sie entscheiden bei diesem Schritt also, dass der Systemzustand eines Rechners auf seinem Betriebssystem basiert werden sollte . Älteren Betriebssystemen werden in der Regel niedrigere **Betriebssystembewertung**sprozentsätze zugewiesen.
- Sie können die **Patch-Bewertung**skriterien ändern.

Hinweis: Ticketing wird bei der Berechnung der Netzwerkleistungsbewertung ignoriert.

Patch-Bewertung – Diese Bewertung wird anhand der durchschnittlichen Anzahl fehlender Patches auf jedem Rechner berechnet. Jeder Rechner wird wie folgt basierend auf der Anzahl fehlender Patches bewertet:

Voll gepatcht	100%
Es fehlen 1-2 Patches	75%
Es fehlen 3-5 Patches	50%
Es fehlen > 5 Patches	25%
Nicht gescannte Rechner	0%

Betriebssystembewertung – Moderne Betriebssysteme erhalten eine höhere Bewertung als ältere Betriebssysteme. Die Betriebssystembewertung insgesamt ist ein Durchschnitt der Bewertung aller Rechner und wird folgendermaßen berechnet:

Win7/Vista/2008	100%
XP/2003	100%
2000	75%
Apple OS	100%
Alle anderen	0%

Hinweis: Die Gewichtung der Betriebssystembewertung kann angepasst werden. Sie können die Betriebssystembewertung, die Sie Win7, Vista, 2008, 2003, XP und 2000 gegeben haben, einzeln gewichten. Geben Sie die Gewichtungen (zwischen 0 und 100 %) in die vier Spalten ein, die normalerweise für die Prozentbewertung verwendet werden. Alle älteren Betriebssysteme erhalten eine Gewichtung von Null. Falls Sie eine große Anzahl von älteren Betriebssystemen verwende, sollten Sie die Betriebssystembewertung deaktivieren.

Plattenbewertung – Volle Festplatten können die Leistung Ihres Systems stark beeinträchtigen. Aus diesem Grund wird der belegte Festplattenspeicher bei der Gesamtbewertung des Systems berücksichtigt. Die Plattenbewertung wird folgendermaßen berechnet:

0% bis 65% voll	100%
65% bis 75% voll	75%
75% bis 85% voll	50%
85 % bis 95 % voll	25%
100% voll	0%

Ticketbewertung – Überfällige Tickets, die Rechnern zugewiesen wurden, werden folgendermaßen

bewertet:

0 überfällig	100%
1 oder 2 überfällig	75%
3 bis 5 überfällig	50%
6 bis 10 überfällig	25%
mehr als 10 überfällig	0%

> **Hinweis:** Das System löscht keine Tickets beim Löschen von Rechner-IDs. Im Ticketübersichtsdiagramm werden Tickets aufgeführt, die dem Rechner-ID-/Rechnergruppen-Filter entsprechen. Da keine Rechnerdaten für gelöschte Rechner-IDs existieren, sind in dieser Tabelle keine Ansichten verfügbar.

Ereignisprotokoll-Bewertung – Überwachte Ereignisprotokollmeldungen können potenzielle Systemprobleme darstellen. Die Anzahl der Ereignisprotokollmeldungen, die von jedem Rechner über den vorgegebenen Zeitraum generiert werden, werden folgendermaßen bewertet:

0 Meldungen	100%
1 bis 4 Meldungen	75%
5 bis 10 Meldungen	50%
11 bis 20 Meldungen	25%
mehr als 20 Meldungen	0%

Sicherungsbewertung – Zählt die Tage, seitdem die letzte Sicherung ausgeführt wurde. Je älter die Sicherung ist, desto niedriger ist die Bewertung.

0 bis 3 Tage seit der letzten Sicherung	100%
4 bis 7 Tage seit der letzten Sicherung	75%
8 bis 14 Tage seit der letzten Sicherung	50%
15 bis 30 Tage seit der letzten Sicherung	25%
mehr als 30 Tage seit der letzten Sicherung	0%

Alarmbewertung – Je weniger Alarme generiert werden, desto höher ist die Bewertung.

0 bis 3 Alarme	100%
4 bis 9 Alarme	75%
10 bis 19 Alarme	50%
20 oder mehr Alarme	25%

Bewertung der Workstation-Laufzeit – Je größer der Prozentsatz der derzeit laufenden Workstations, desto höher ist die Bewertung.

90	100%
80	75%
70	50%
60	25%

Bewertung der Server-Laufzeit – Je größer der Prozentsatz der derzeit laufenden Server, desto höher ist die Bewertung.

99	100%
97	75%
95	50%
90	25%

Sicherheitsbewertung – Nicht behobene Bedrohungen stellen potenzielle Systemprobleme dar. Die Anzahl der nicht behandelten Bedrohungen, die von jedem Rechner über den vorgegebenen Zeitraum generiert wurden, werden folgendermaßen bewertet:

0 nicht behandelte Bedrohungen	100%
1 bis 4 nicht behandelte Bedrohungen	75%
5 bis 10 nicht behandelte Bedrohungen	50%
11 bis 19 nicht behandelte Bedrohungen	25%
mehr als 20 nicht behandelte Bedrohungen	0%

> **Hinweis:** Die **Sicherheitsbewertung** wird nur angezeigt, wenn Sie das Endpoint Security-Zusatzmodul separat erworben haben.

Antivirus-Ergebnis – Die Antivirusbewertung ist ein zusammengesetztes Ergebnis, das für jeden einzelnen Rechner folgendermaßen gewichtet wird:

- **Prozentsatz der Antivirusinstallation – 40 %** – Ist ein Antivirusprogramm auf dem Rechner installiert?
- **Vollständige Scans während der Periode – 40 %** – Wurde zumindest ein Antivirus-Scan während des Zeitraums durchgeführt?
- **Aktive Bedrohungen – 20 %** – Wurden null Bedrohungen während des Zeitraums erkannt?

Nachdem die Antivirus-Bewertung eines jeden Rechners ermittelt wurde, werden die Ergebnisse in folgende anpassbare Prozentsatz-Buckets gruppiert: 100%, 75%, 50%, 25%.

> **Hinweis:** Das **Antivirus-Ergebnis** wird nur angezeigt, wenn Sie das **Antivirus**-Zusatzmodul separat erworben haben.

AntiMalware-Bewertung – Die **AntiMalware**-Bewertung ist ein zusammengesetztes Ergebnis, das für jeden einzelnen Rechner folgendermaßen gewichtet wird:

- **Prozentsatz der Antivirusinstallation – 40 %** – Ist **AntiMalware** auf dem Rechner installiert?
- **Vollständige Scans während der Periode – 40 %** – Wurde zumindest ein **AntiMalware**-Scan während des Zeitraums durchgeführt?
- **Aktive Bedrohungen – 20 %** – Wurden null Bedrohungen während des Zeitraums erkannt?

Nachdem die **AntiMalware**-Bewertung eines jeden Rechners ermittelt wurde, werden die Ergebnisse in folgende anpassbare Prozentsatz-Buckets gruppiert: 100%, 75%, 50%, 25%.

> **Hinweis:** Die **AntiMalware-Bewertung** wird nur angezeigt, wenn Sie das **AntiMalware**-Zusatzmodul separat erworben haben.

Verfahrensbewertung – Verfahren stellen einen wiederkehrenden vorteilhaften Service für einen Rechner zur Verfügung. Je öfter Sie das Verfahren ausführen, desto besser ist wahrscheinlich der Systemzustand des Rechners. Je mehr Zeit verstrichen ist, seit das Verfahren das letzte Mal ausgeführt wurde, desto niedriger ist die Bewertung. Die gewichteten Schwellenwerte für die Verfahrensbewertung zählen die Anzahl der Tage, seit das Verfahren zum letzten Mal auf den Rechnern ausgeführt wurde. Die Standardwerte ergeben die folgende Bewertung:

1	0 bis 3 Tage seit das Verfahren das letzte Mal ausgeführt wurde	100%
2	4 bis 9 Tage seit das Verfahren das letzte Mal ausgeführt wurde	75%
3	10 bis 19 Tage seit das Verfahren das letzte Mal ausgeführt wurde	50%
4	20 oder mehr Tage seit das Verfahren das letzte Mal ausgeführt wurde	25%

Hinweis: Sie müssen mindestens ein * in das Feld Beschreibungsfilter eingeben, um Ergebnisse zu erhalten.

KDS – Domänen-Aktivität

Info Center > Reporting > Berichte > KDS - Domänen-Aktivität

- Wird nur angezeigt, wenn das Discovery-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Domänen-Aktivität** wird ein Bericht der für **Discovery** sichtbaren Domänen-Konfigurationsänderungen generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

Filtern Sie nach Datumsbereich.

- **Startdatum/-zeit**
- **Enddatum/-zeit**

Aktivität

Filtern Sie nach dem Typ des Objekts und der Aktionen, die an diesen Objekten ausgeführt werden.

- **Objekttypen**: `Computer`, `Kontakt`, `Container`, `Domäne`, `Gruppe`, `Organisationseinheit`, `Benutzer`
- **Aktionstypen**: `Erstellt`, `Aktualisiert`, `Gelöscht`

Datensicherung-Zusammenfassung

Info Center > Reporting > Berichte > Audit - Datensicherung-Zusammenfassung

- Wird nur angezeigt, wenn das Data Backup-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Datensicherung-Zusammenfassung** wird ein zusammenfassender Bericht der **Data Backup**-Aktivitäten nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Rechner ohne Daten miteinbeziehen** – Bei Aktivierung dieses Kontrollkästchens werden Rechner ohne Backups mit einbezogen.
- **Detail anzeigen** – Bei Aktivierung dieses Kontrollkästchens werden alle Backup-Aktivitäten für einen Rechner angezeigt. Bei Nichtaktivierung wird nur die letzte Backup-Aktivität angezeigt.

Datensicherungsnutzung im Zeitverlauf

Info Center > Reporting > Berichte > KOB - Datensicherungsnutzung im Zeitverlauf

- Wird nur angezeigt, wenn das Data Backup-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Datensicherungsnutzung im Zeitverlauf** wird ein Bericht der **Data Backup**-Nutzung nach Zeitperiode generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Rechner ohne Daten miteinbeziehen** – Bei Aktivierung dieses Kontrollkästchens werden Rechner ohne Backups mit einbezogen.
- **Zeitperiode auswählen** – `Täglich`, `Wöchentlich`, `Monatlich`, `Vierteljährlich`, `Jährlich`.
- **Auslastungstyp auswählen** – `Spitzenauslastung anzeigen`, `Durchschnittliche Auslastung anzeigen`.

Protokolle – Administratoranmerkungen

Info Center > Reporting > Berichte > Protokolle - Administratorhinweise

Mit der Berichtsdefinition **Administratoranmerkungen** werden Berichte mit **Administratoranmerkungen** *(siehe 14)* generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen
- **Einträge anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Agent-Protokoll

Info Center > Reporting > Berichte > Protokolle - Agent-Protokolle

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Agent-Protokoll** *(siehe 35)* wird ein Bericht der Agent-Protokolleinträge nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen
- **Einträge anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Agent-Verfahren

Info Center > Reporting > Berichte > Protokolle - Agent-Verfahren

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Skripting** wird ein Bericht aller system- und benutzerdefinierten Agent-Verfahren generiert, die auf jeder Rechner-ID ausgeführt werden, einschließlich des Erfolgs- oder Fehlerstatus der einzelnen Agent-Verfahren sowie des VSA-Benutzers, der sie geplant hat.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum die in den Bericht eingeschlossen werden sollen
- **Namenfilter für Agent-Verfahren** – Filtert die Einträge nach Namen des Agent-Verfahrens.
- **Administratorfilter (Admin, der das Agent-Verfahren plante)** – Filtert die Einträge nach dem VSA-Benutzer, der das Agent-Verfahren geplant hat.
- **Einträge anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Alarmprotokoll

Info Center > Reporting > Berichte > Protokolle - Alarmprotokoll

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Alarmprotokoll** wird ein Bericht der Alarmprotokolleinträge nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Meldungstyp für die Anzeige auswählen** – Filtert nach **Meldungstypen** *(siehe 622)*.
- **Filter für E-Mail-Adresse, an die Meldung gesendet wurde** – Filtert nach dem E-Mail-Empfänger des Alarms.
- **Meldungs-Betreffzeilenfilter** – Filtert nach der E-Mail-Betreffzeile des Alarms.
- **Alarm-Nachrichteninhaltsfilter** – Filtert nach dem E-Mail-Nachrichteninhalt des Alarms.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Konfigurationsänderungen

Info Center > Reporting > Berichte > Protokolle - Konfigurationsänderungen

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Konfigurationsänderungen** wird ein Bericht der Änderungen an den

VSA-Einstellungen generiert, die an jeder Rechner-ID vorgenommen wurden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen
- **Einträge anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Ereignisprotokolle

Info Center > Reporting > Berichte > Protokolle - Ereignisprotokolle

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Ereignisprotokolle** wird ein Bericht der **Ereignisprotokoll** *(siehe 618)*daten generiert, die von Windows für eine bestimmte Rechner-ID erfasst wurden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Protokolleinträge für die letzten N Tage anzeigen** – Anzahl der Tage, rückwirkend seit dem aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen
- **Ereignistyp wählen** – Filtert den Bericht nach Ereignisprotokolltyp.
- **Nach Ereignissatz filtern** – Filtert den Bericht nach dem ausgewählten Ereignissatz. Andernfalls werden alle Ereignisse gemeldet.
- **Ereigniskategorien** – Filtert den Bericht nach Ereigniskategorie.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Ereignisprotokollfrequenz

Info Center > Reporting > Berichte > Protokolle - Ereignisprotokollhäufigkeit

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Ereignisprotokollfrequenz** wird ein Bericht der *häufigsten Ereignis-IDs* im **Ereignisprotokoll** *(siehe 618)*daten generiert, die von Windows für eine bestimmte Rechner-ID erfasst wurden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Berichtsparameter

- **Die <N> häufigsten Ereignis-IDs für jede Rechner-ID auswählen** – Wählen Sie die Anzahl der häufigsten Ereignis-IDs aus.
- **Ereignistyp wählen** – Filtert den Bericht nach Ereignisprotokolltyp.
- **Ereigniskategorien** – Filtert den Bericht nach Ereigniskategorie.

- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Protokoll-Monitoring

Info Center > Reporting > Berichte > Protokolle - Protokoll-Monitoring

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Protokoll-Monitoring** wird ein Bericht der Protokolleinträge zum **Protokoll-Monitoring** *(siehe 626)* generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Berichtsparameter

- **Protokolldateianalyse wählen** – Filtert den Bericht nach Protokollanalysedefinition.
- **Einträge anzeigen, die folgender Beschreibung entsprechen** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Netzwerkstatistik-Protokoll

Info Center > Reporting > Berichte > Protokolle - Netzwerkstatistik-Protokoll

- Über Info Center > Reporting > Berichte > Audit > Netzwerkstatistik *(siehe 208)* werden die *Hauptverbraucher* von Netzwerkbandbreite identifiziert.
- Zugehörige Informationen werden über System > Statistiken *(siehe 442)* bereitgestellt.
- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Netzwerkstatistikprotokoll** wird ein Bericht der **Netzwerkstatistik** *(siehe 208)* nach Rechner-ID generiert.

> **Hinweis:** Für dieses Protokoll muss der Treiber Audit > **Netzwerkzugriff** *(siehe 84)* aktiviert sein. Dieser Treiber fügt sich in den TCP/IP-Stapel ein, um den auf dem TCP/IP-Protokoll basierenden Datenverkehr nach Anwendung zu messen. Er ist standardmäßig *deaktiviert*.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum die in den Bericht eingeschlossen werden sollen
- **Anwendungen anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Protokolle – Fernsteuerung

Info Center > Reporting > Berichte > Protokolle - Fernsteuerung

- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition **Fernsteuerung** wird ein Bericht der Fernsteuerungssitzungen nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen
- **Einträge anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Mobile Geräte – Geräteanwendungen

Info Center > Reporting > Berichte > Mobile Geräte - Geräteanwendungen

- Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Geräteanwendungen** wird ein Bericht generiert, in dem die auf einem Gerät installierten Anwendungen aufgeführt sind.

Filter- und Sortierungsparameter

- **Betriebssystem-Typ** – `Android`, `Apple`
- **Hersteller** – Der Hersteller der Gerätehardware.
- **Original-Netzbetreiber** – Die Hauptnetzbetreiber für Geräte.
- **Aktueller Netzbetreiber** – Die Netzbetreiber, deren Services von Geräten derzeit verwendet werden.
- **Anwendungsname** – Der Name der auf Geräten installierten Anwendung.

Mobile Geräte – Gerätestatus

Info Center > Reporting > Berichte > Mobile Geräte - Gerätestatus

- Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.

Mit der Berichtsanwendung **Gerätestatus** wird ein Bericht generiert, in dem die Status eines jeden Geräts aufgeführt sind.

Filter- und Sortierungsparameter

- **Mobilgerätestatus** – *Nachstehend werden nur die gängigsten Befehle aufgeführt.*
  - `Eingeladen` – Dem Benutzer wird eine Einladung zugesandt, die Kaseya Agent-App auf dem Gerät des Benutzer zu installieren.
  - `Normal` – Die App ist installiert und funktioniert einwandfrei.
  - `Befehl ausstehend` – Aus dem Gerät des Benutzers steht ein Befehl für die Kaseya-Agent-App aus.
- **Betriebssystem-Typ** – `Android`, `Apple`
- **Verfolgen** – `True`, `False`

Mobile Geräte – Geräteübersicht

Info Center > Reporting > Berichte > Mobile Geräte - Geräteübersicht

- Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Geräteübersicht** wird ein Übersichtsbericht aller Auditinformationen von ausgewählten Rechnern generiert.

Filter- und Sortierungsparameter

- **Mobilgerätestatus** – *Nachstehend werden nur die gängigsten Befehle aufgeführt.*
  - `Eingeladen` – Dem Benutzer wird eine Einladung zugesandt, die Kaseya Agent-App auf dem Gerät des Benutzer zu installieren.
  - `Normal` – Die App ist installiert und funktioniert einwandfrei.
  - `Befehl ausstehend` – Aus dem Gerät des Benutzers steht ein Befehl für die Kaseya-Agent-App aus.
- **Betriebssystem-Typ** – `Android`, `Apple`
- **Hersteller** – Der Hersteller der Gerätehardware.
- **Original-Netzbetreiber** – Die Hauptnetzbetreiber für Geräte.

Anzuzeigende Detailtabellen

- **Detail zu Betriebssystem anzeigen**
- **Details für Geräteinfo anzeigen**
- **Plattformdetaildaten anzeigen**
- **Details für Original-Netzwerk anzeigen**
- **Details für aktuelles Netzwerk anzeigen**

Anzuzeigende Detailgrafiken

- **Diagramm für Mobilgerätestatus anzeigen**
- **Diagramm für Betriebssystemart anzeigen**
- **Herstellerdiagramm anzeigen**
- **Diagramm für Original-Netzbetreiber anzeigen**
- **Diagramm für aktuellen Netzbetreiber anzeigen**

Mobile Geräte – Verlorene Geräte

Info Center > Reporting > Berichte > Mobile Geräte - Verlorene Geräte

- Wird nur angezeigt, wenn das Mobile Device Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Verlorene Geräte** wird ein Bericht aller verlorenen Geräte generiert.

Zeitrahmen

- **Von** – Filtert den Datumsbereich des Berichts nach diesem Startdatum.
- **Bis** – Filtert den Datumsbereich des Berichts nach diesem Enddatum.

Monitoring – Protokolle

Info Center > Reporting > Berichte > Monitoring - Protokolle

Die Berichtsdefinition **Protokolle** stellt einen einzelnen Zugriffspunkt zum Generieren jeder anderen Art von Protokollbericht bereit. Sämtliche Parameter für alle Protokollberichte werden auf der Registerkarte Parameter bereitgestellt. Beim Angeben eines Protokollberichts sind nur die Parameter, die diese Art von Protokollbericht unterstützen, darauf anwendbar. Welche Parameterfelder Anwendung finden, erfahren Sie in den folgenden Abschnitten zum Thema Protokolle.

- **Protokolle – Agent-Protokoll** *(siehe 218)*
- **Protokolle – Konfigurationsänderungen** *(siehe 219)*
- **Protokolle – Netzwerkstatistik** *(siehe 221)*
- **Protokolle – Ereignisprotokolle** *(siehe 220)*

   - Anwendungs-Ereignisprotokoll
   - Sicherheits-Ereignisprotokoll
   - System-Ereignisprotokoll
   - Alle Ereignis-Protokolle
- **Protokolle – Agent-Verfahren** *(siehe 219)*
- **Protokolle – Administratoranmerkungen** *(siehe 218)*
- **Protokolle – Alarmprotokoll** *(siehe 219)*
- **Protokolle – Fernsteuerung** *(siehe 222)*
- **Protokolle – KES-Protokoll** *(siehe 229)*

Monitoring – 95. Perzentil-Monitoring

Info Center > Reporting > Berichte > Monitoring - 95. Perzentil-Monitoring

Mit der Berichtsdefinition **95. Perzentil-Monitoring** werden zwei Daten angegeben und das 95. Perzentil berechnet, mit anderen Worten, zu 95 % der Zeit liegt der Wert unter dem im Bericht berechneten Wert. Identifiziert die *typischen* Bandbreitenanforderungen für einen Rechner oder ein Gerät, die knapp unter den Spitzenwert-Ereignissen liegen. Der Bericht unterstützt SLA- und Planungskalkulationen.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Berichtsparameter

- **Wählen Sie das Monitor-Set oder SNMP-Set aus**
- **Durchschnittswert** – Wählen Sie den Durchschnittswert aus, der in dem Bericht verwendet werden soll.
- **Zähler/MIB-Objekte auswählen, die dem Bericht hinzugefügt werden sollen** – Wählen Sie spezifische Zähler in dem ausgewählten Monitor-Set oder bestimmte MIB-Objekte im ausgewählten SNMP-Set aus, die in den Bericht eingeschlossen werden sollen.

Monitoring – Monitor-Aktionsprotokoll

Info Center > Reporting > Berichte > Monitoring - Monitor-Aktionsprotokoll

Mit der Berichtsdefinition **Monitor-Aktionsprotokoll** wird ein Bericht der **Meldungsbedingungen** *(siehe 621)* und der Aktionen, die als Reaktion auf jede Meldungsbedingung ergriffen werden, generiert.

Ein Benutzer kann Monitor-Sets, SNMP-Sets, Meldungen, Systemprüfungen oder Protokoll-Monitoring bestimmten Rechner-IDs zuweisen, *ohne das Kontrollkästchen "Alarm erstellen" zu aktivieren*. In diesem Fall wird trotzdem ein **Monitor-Aktionsprotokoll**-Eintrag erstellt. Anhand dieser Protokolle kann ein VSA-Benutzer *Meldungen* überprüfen, ganz gleich, ob er durch die Erstellung eines Alarms, eines Tickets oder per E-Mail speziell darüber benachrichtigt wurde oder nicht. Sie können über Info Center > Reporting > Berichte > Monitoring > **Monitor-Aktionsprotokoll** *(siehe 224)* generieren.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Berichtsparameter

- **Monitor-Typ** – `Zähler`, `Prozess`, `Dienst`, `SNMP`, `Meldung`, `Systemprüfung`, `Sicherheit` oder `Protokoll-Monitoring`.
- **Nachrichtenfilter** – Geben Sie eine Zeichenfolge ein, um Alarme nach dem Nachrichtentext zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Nach Zeitpunkt des Protokollereignisses sortieren** – `Aufsteigend`, `Absteigend`

Monitoring – Monitor-Alarmübersicht

Info Center > Reporting > Berichte > Monitoring - Monitor-Alarm-Übersicht

- Über Info Center > Reporting > Berichte > Monitoring > Monitor-Aktionsprotokoll *(siehe 224)* können Sie Meldungs*bedingungen* überprüfen, ohne Alarme zu generieren.

Mit der Berichtsdefinition **Monitor-Alarmübersicht** wird ein Bericht der erstellten Alarme nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Berichtsparameter

- **Monitor-Typ** – `Zähler`, `Prozess`, `Dienst`, `SNMP`, `Meldung`, `Systemprüfung`, `Sicherheit` oder `Protokoll-Monitoring`.
- **Alarmtyp** – `Alarm`, `Trending`
- **Nachrichtenfilter** – Geben Sie eine Zeichenfolge ein, um Alarme nach dem Nachrichtentext zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Nach Zeitpunkt des Protokollereignisses sortieren** – `Aufsteigend`, `Absteigend`
- **Nachricht mit jedem Alarm anzeigen** – Schließen Sie für jeden generierten Alarm eine detaillierte Nachricht ein.

Monitoring – Monitorkonfiguration

Info Center > Reporting > Berichte > Monitoring - Monitorkonfiguration

Mit der Berichtsdefinition **Monitorkonfiguration** wird ein Bericht der Konfigurationsdetails jedes einer Rechner-ID zugewiesenen Monitor-Sets bzw. jedes einem Gerät zugewiesenen SNMP-Sets generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Nur zugewiesene Sets auflisten** – Wenn diese Option aktiviert ist, werden nur die Rechner-ID zugewiesenen Monitor-Sets bzw. Geräten zugewiesene SNMP-Sets angezeigt.
- **Anzuzeigende Sets auswählen** – Wählen Sie im linken Fensterbereich Sets aus und klicken Sie auf die Schaltfläche >, um sie in den rechten Fensterbereich zu verschieben.

Monitoring – Monitor-Protokoll

Info Center > Reporting > Berichte > Monitoring - Monitor-Protokoll

Mit der Berichtsdefinition **Monitor-Protokoll** wird ein Bericht der Monitor-Protokolldaten für Monitor-Sets und SNMP-Sets nach Rechner-ID, Zähler und MIB-Objekt generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Geben Sie die Anzahl der Protokolleinträge für jeden Zähler und jeden Rechner an**
- **Zählerprotokolldaten anzeigen**
- **Serviceprotokolldaten anzeigen**
- **Prozess-Logdaten anzeigen**
- **SNMP-Protokolldaten anzeigen**

Monitoring – Monitor-Set

Info Center > Reporting > Berichte > Monitoring - Monitor-Set

Mit der Berichtsdefinition **Monitor-Set** wird ein Bericht der Monitor-Protokolls für ein einzelnes Monitor-Set oder SNMP-Set nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Monitor-Set auswählen** – Wählen Sie ein einzelnes Monitor-Set oder SNMP-Set aus.
- **Letzte anzeigen** – Anzahl der Perioden rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen.

Monitoring – Monitor-Trend

Info Center > Reporting > Berichte > Monitoring - Monitor-Trend

Mit der Berichtsdefinition **Monitor-Trend** wird ein Bericht der Monitor-Protokolls für einen einzelnen Monitor-Set-Zähler oder ein einzelnes SNMP-Set-MIB-Objekt nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Monitor-Set auswählen** – Wählen Sie ein einzelnes Monitor-Set oder SNMP-Set aus.
- **Zähler auswählen** – Wählen Sie einen Zähler im ausgewählten Monitor-Set oder ein MIB-Objekt im ausgewählten SNMP-Set aus.
- **Letzte anzeigen** – Anzahl der Perioden rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen.

Monitoring – Laufzeit-Historie

Info Center > Reporting > Berichte > Monitoring - Betriebszeit-Historie

Mit der Berichtsdefinition **Laufzeit-Historie** wird ein grafischer Bericht generiert, in dem Folgendes dargestellt wird:

- Wann jeder Rechner eingeschaltet wurde
- Wann jeder verwaltete Rechner mit dem Netzwerk verbunden wurde
- Alle anormalen Shutdowns

Wenn Sie die Maus über ein beliebiges Segment auf dem Diagramm führen, wird ein Tooltip mit der exakten Start- und Endzeit dieses Segments angezeigt.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **N Tage der Rechnerlaufzeit und Online-Zeit anzeigen** – Anzahl der Tage bis zum aktuellen Datum, die in den Bericht eingeschlossen werden sollen
- **Alle Zeiten in der lokalen Zeitzone jedes Agents anzeigen** – Alle Ereignisse werden in der lokalen Zeit des Rechners aufgeführt.
- **Alle Zeiten in der Zeitzone des Systemservers anzeigen** – Alle Ereignisse werden in der Zeitzone des Kaseya Server dargestellt.

Patch – Patch-Management

Info Center > Reporting > Berichte> Patch-Verwaltung

- Über Patch-Verwaltung > Patch-Status, Rechnerhistorie, Rechner-Update und Patch-Aktualisierung werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Patch-Management** wird ein Bericht generiert, in dem der Patch-Status aller ausgewählten Rechner-IDs aufgelistet wird. Berichte können nach Patch-Kategorie oder Knowledge Base-Artikelnummer gefiltert werden. Die Berichte können auch Patches einschließen, die von der Patch-Richtlinie abgelehnt wurden. Berichte schließen Links zu KB-Artikeln ein.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Optionen anzeigen

- **Rechner-Patch-Übersichtskreisdiagramm** – Zeigt ein Kreisdiagramm mit der Anzahl der Rechner, für die Folgendes gilt:
  - Vollständig gepatchte Systeme
  - Mit 1 oder 2 fehlenden Patches
  - Mit 3, 4 oder 5 fehlenden Patches
  - Mit mehr als 5 fehlenden Patches
  - Ist niemals gescannt worden
- **Rechner-Patch-Übersichtstabelle** – Zeigt eine Tabelle mit einer Übersicht über die Patches auf einem Rechner an.
- **Häufigkeitsbalkendiagramm fehlender Patches** – Zeigt ein Balkendiagramm an, das illustriert, welche Patches auf den meisten Rechnern fehlen.
- **Tabelle der fehlenden Patches** – Dies ist ein zusammengesetzter Bericht, der alle Patches aufführt, die auf allen oder einigen Rechnern in der ausgewählten Gruppe fehlen. Die Tabelle enthält einen Abschnitt für den fehlenden Patch mit den folgenden Angaben: Patch-ID, Knowledge Base-Artikelnummer und Patch-Titel. Wenn `Anzeigen (Rechner miteinbeziehen, auf denen jedes Patch fehlt)` ausgewählt ist, werden im Bericht alle Rechner-IDs, denen das Patch fehlt, aufgeführt.
- **Tabelle der installierten Patches** – Dies ist ein zusammengesetzter Bericht, der alle Patches aufführt, die auf allen oder einigen Rechnern in der ausgewählten Gruppe installiert sind. Diese Tabelle enthält die entgegengesetzten Daten von **Tabelle der fehlenden Patches**. Die Tabelle enthält einen Abschnitt für den installierten Patch mit den folgenden Angaben: Patch-ID, Knowledge Base-Artikelnummer und Patch-Titel. Wenn `Anzeigen (Rechner miteinbeziehen, auf denen jedes Patch fehlt)` ausgewählt ist, werden im Bericht alle Rechner-IDs, für die das Patch installiert wurde, aufgeführt.
- **Patch-Status für jeden Rechner** – Für jede Rechner-ID wird eine Liste der installierten und fehlenden Patches aufgeführt. Patches werden nach Anwendung gruppiert. Wenn `Anzeigen (einschließlich Titel für jedes Patch)` ausgewählt ist, werden die Titel zur Beschreibung der Patches ebenfalls mit aufgeführt.
- **Fehlende Patches für jeden Rechner** – Für jede Rechner-ID wird eine Liste der fehlenden Patches angezeigt. Patches werden nach Anwendung gruppiert. Wenn `Anzeigen (einschließlich Titel für jedes Patch)` ausgewählt ist, werden die Titel zur Beschreibung der Patches ebenfalls mit aufgeführt.

- **Patches, die in den letzten <N> Tagen installiert wurden** – Für jede Rechner-ID wird eine Liste der Patches angezeigt, die während der im Textfeld angezeigten Anzahl von Tagen installiert wurden. Wenn `Anzeigen (einschließlich Titel für jedes Patch)` ausgewählt ist, werden die Titel zur Beschreibung der Patches ebenfalls mit aufgeführt.

Filter

- **Nummern der Knowledge Base-Artikel und/oder Sicherheitsberichte** – Geben Sie eine durch Kommata getrennte Liste von Nummern von Knowledge Base-Artikeln und/oder Sicherheitsberichten ein, um einen Bericht zu generieren, in dem nur die Patches für diese Nummern aufgelistet werden.
- **Standardfilter** – Wählen Sie die Filterkriterien für den Patch-Bericht aus.
- **Von der Patch-Bestätigungsregel abgelehnte Patches zeigen** – Standardmäßig werden nur fehlende Patches, deren Installation bestätigt wurde, in diesem Bericht aufgeführt. Aktivieren Sie das Kontrollkästchen, um die **Patch-Bestätigungsregel** *(siehe 624)* zu übergehen und alle Patches, ob bestätigt oder abgelehnt, mit einzuschließen

Policy Management – Agent-Richtlinienstatus

Info Center > Reporting > Berichte > Policy Management - Agent-Richtlinienstatus

- Wird nur angezeigt, wenn das Policy Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Agent-Richtlinienstatus** wird ein Richtlinienstatusbericht generiert. Dies kann nach Folgendem gefiltert werden:

- **Agent-Richtlinienstatus**
- **Richtlinien-Objekttyp**
- **Richtlinien-Objektstatus**

Policy Management – Richtliniendaten & Zuordnung

Info Center > Reporting > Berichte > Policy Management - Richtliniendaten & Zuordnung

- Wird nur angezeigt, wenn das Policy Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Richtliniendaten & Zuordnung** wird ein Bericht zu Richtliniendaten und Zuordnungen generiert. Dies kann nach Folgendem gefiltert werden:

- **Richtlinienstatus**
- **Richtlinien-Objekttyp**

Sicherheit – Konfiguration

Info Center > Reporting > Berichte > Sicherheit > Konfiguration

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Ähnliche Informationen werden über Sicherheit > Sicherheitsstatus, Protokolle anzeigen und Bedrohungen anzeigen bereitgestellt.

Mit der Berichtsdefinition **Sicherheit – Konfiguration** werden Berichte für die folgenden Arten von Sicherheitsdaten generiert, die vom VSA gepflegt werden.

- Installationszeit
- Installer
- Version
- Ablaufdatum der Lizenz
- Zugewiesenes Profil
- Profildetails
- Alarmeinstellungen

Sicherheit – Aktuelle Bedrohungen

Info Center > Reporting > Berichte > Sicherheit > Aktuelle Bedrohungen

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Ähnliche Informationen werden über Sicherheit > Sicherheitsstatus, Protokolle anzeigen und Bedrohungen anzeigen bereitgestellt.

Mit der Berichtsdefinition **Sicherheit – Aktuelle Bedrohungen** werden Berichte für die folgenden Arten von Sicherheitsdaten generiert, die vom VSA gepflegt werden.

- Übersicht
- Übersicht über Bedrohungskategorie
- Aktuelle Bedrohungen

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Sicherheit – Historische Bedrohungen

Info Center > Reporting > Berichte > Sicherheit > Historische Bedrohungen

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Ähnliche Informationen werden über Sicherheit > Sicherheitsstatus, Protokolle anzeigen und Bedrohungen anzeigen bereitgestellt.

Mit der Berichtsdefinition **Sicherheit – Historische Bedrohungen** werden Berichte für die folgenden Arten von Sicherheitsdaten generiert, die vom VSA gepflegt werden.

- Übersicht
- Übersicht über Bedrohungskategorie
- Aktuelle Bedrohungen

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Sicherheit – KES-Protokoll

Info Center > Reporting > Berichte > Sicherheit > KES-Protokoll

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Unter Agent > Agent-Protokolle *(siehe 35)* werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition KES-Protokoll wird ein Bericht der Endpoint Security-Protokolleinträge nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen
- **Einträge anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Leistungsabrechnung – Zuletzt abgerechnete Rechnungen

Info Center > Reporting > Berichte > Leistungsabrechnung – Zuletzt abgerechnete Rechnungen

- Wird nur angezeigt, wenn das Service Billing-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Zuletzt abgerechnete Rechnungen** wird ein Bericht generiert, in dem die abgerechneten Rechnungen aufgeführt sind.

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Leistungsabrechnung – Kundenauftragsübersicht

Info Center > Reporting > Berichte > Leistungsabrechnung – Kundenauftragsübersicht

- Wird nur angezeigt, wenn das Service Billing-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Kundenauftragsübersicht** wird ein zusammenfassender Bericht der Verkaufsaufträge generiert.

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Leistungsabrechnung – Nicht berechneter Umsatz nach Kunden

Info Center > Reporting > Berichte > Leistungsabrechnung – Nicht berechneter Umsatz nach Kunden

- Wird nur angezeigt, wenn das Service Billing-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Nicht berechneter Umsatz nach Kunden** wird ein detaillierter Bericht oder eine Übersicht über den nicht berechneten Umsatz nach Kunden generiert.

Parameter

- **Detailliert**
- **Übersicht**

Leistungsabrechnung – Nicht berechneter Umsatz nach Positionstyp

Info Center > Reporting > Berichte > Leistungsabrechnung - Nicht berechneter Umsatz nach Positionstyp

- Wird nur angezeigt, wenn das Service Billing-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Nicht berechneter Umsatz nach Positionstyp** wird ein detaillierter Bericht oder eine Übersicht über den nicht berechneten Umsatz nach Positionstyp generiert.

Parameter

- **Detailliert**
- **Übersicht**

Leistungsabrechnung – Arbeitsauftragsübersicht

Info Center > Reporting > Berichte > Leistungsabrechnung - Arbeitsauftragsübersicht

- Wird nur angezeigt, wenn das Service Billing-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Arbeitsauftragsübersicht** wird ein zusammenfassender Bericht der Arbeitsaufträge generiert.

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Service Desk – Benutzerdefinierte Tickets

Info Center > Reporting > Berichte > Service Desk - Benutzerdefinierte Tickets

- Wird nur angezeigt, wenn das Service Desk-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Benutzerdefinierte Tickets** wird ein Bericht generiert, in dem Übersichtsinformationen und Details von **Service Desk**-Tickets angezeigt werden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Allgemein

- **Service-Desk**
- **Anmerkungen-/Zusammenfassung-/Absenderfilter** – Führt nur Tickets oder Ticketzahlen auf, die diese Zeichenfolge in einer Anmerkung, einer Zusammenfassungs- oder Absenderinformationenzeile enthalten. Verwenden Sie * als Stellvertreterzeichen.
- **Alle Tickets anzeigen** – Wenn aktiviert, werden alle Tickets einzeln aufgeführt.
- **Anmerkungen mit jedem Ticket anzeigen** – Wenn aktiviert, werden mit jedem Ticket Anmerkungen angezeigt.

- **Ausgeblendete Anmerkungen verbergen** – Wenn aktiviert, werden ausgeblendete Anmerkungen verborgen.
- **Ticketstatusdiagramm für jeden Administrator anzeigen** – Zeigt ein separates Ticketstatus-Balkendiagramm für jeden Benutzer und für nicht zugewiesen an.
- **Tortendiagramm für alle Datenspalten der gewählten Ticketkategorie anzeigen** – `Bearbeiter`, `Status`, `Priorität`, `Kategorie`, `Unterkategorie`.

Zeitrahmen

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Alle offenen Tickets und solche, die innerhalb der letzten N Tage geschlossen wurden, anzeigen** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Spalten

Werte für alle Service Desk-Definitionen werden in den Dropdown-Listen angezeigt. Sie können mit den Tastenkombinationen `Strg + Klicken` und `Umschalt + Klicken` mehrere Elemente auswählen, sofern nicht anderweitig angegeben.

- **Sortierspalte** – Wählen Sie die Spalte aus, nach der Tickets sortiert werden sollen.
- **Sortierrichtung** – `Aufsteigend`, `Absteigend`.

Filter

- **Administratorfilter** – Es kann nur jeweils ein Element ausgewählt werden.
- **Statusfilter**
- **Prioritätenfilter**
- **Kategoriefilter**
- **Unterkategorie-Filter** – Es werden nur Unterkategorien für ausgewählte Kategorien im **Kategorie.Filter** angezeigt.

Service Desk – Serviceziele

Info Center > Reporting > Berichte > Service Desk - Serviceziele

- *Wird nur angezeigt, wenn das Service Desk-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Serviceziele** wird ein Bericht generiert, in dem Übersichtsinformationen und Ticketdetails in Bezug auf das Erreichen der **Service Desk**-Serviceziele angezeigt werden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Nur Tickets mit Zielen einschließen** – Wenn aktiviert, werden nur Tickets mit Zielen angezeigt.
- **Bericht nach Typ auswählen** – `Serviceziele nach Ticket`, `Ticketnummer`.

- **Sortierspalte** – Wählen Sie die Spalte aus, nach der Tickets sortiert werden sollen.
- **Sortierrichtung** – `Aufsteigend`, `Absteigend`.

Service Desk – Servicestunden

Info Center > Reporting > Berichte > Service Desk - Servicestunden

- *Wird nur angezeigt, wenn das Service Desk-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Servicestunden** wird ein Bericht generiert, in dem Übersichtsinformationen und Ticketdetails in Bezug auf die gearbeiteten **Service Desk**-Stunden angezeigt werden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Nur Tickets mit Zielen einschließen** – Wenn aktiviert, werden nur Tickets mit Zielen angezeigt.
- **Bericht nach Typ auswählen** – `Servicestunden nach Ticket`, `Servicestunden nach Teilnehmer`, `Servicestunden nach Organisation`.
- **Sortierspalte** – Wählen Sie die Spalte aus, nach der Tickets sortiert werden sollen.
- **Sortierrichtung** – `Aufsteigend`, `Absteigend`.

Service Desk – Servicezeiten

Info Center > Reporting > Berichte > Service Desk - Servicezeiten

- *Wird nur angezeigt, wenn das Service Desk-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Servicezeiten** wird ein 12-monatiger Bericht generiert, der bei einem angegebenen Monat und Jahr beginnt und anzeigt, wie viele Tickets erstellt, geschlossen oder gelöst wurden oder innerhalb fester Zeitfenster überfällig sind.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Parameter

- **Monat** – Wählen Sie einen Monat aus.
- **Jahr** – Wählen Sie ein Jahr aus.
- **Erstellte Tickets anzeigen** – Wenn aktiviert, werden erstellte Tickets angezeigt.
- **Geschlossene Tickets anzeigen** – Wenn aktiviert, werden geschlossene Tickets angezeigt.
- **Aufgelöste Tickets anzeigen** – Wenn aktiviert, werden aufgelöste Tickets angezeigt.
- **Überfällige Tickets anzeigen** – Wenn aktiviert, werden überfällige Tickets angezeigt.
- **Ticket-Servicezeit-Detailtabellen anzeigen** – Wenn aktiviert, werden Ticket-Detailtabellen angezeigt.

Service Desk – Serviceumfänge

Info Center > Reporting > Berichte > Service Desk - Serviceumfänge

- *Wird nur angezeigt, wenn das Service Desk-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Serviceumfänge** wird ein 12-monatiger Bericht generiert, der bei einem

angegebenen Monat und Jahr beginnt und anzeigt, wie viele Tickets in jedem Monat zu jedem möglichen Wert in einer angegebenen Ticketspalte gehören.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Parameter

- **Gruppieren nach** – Wählen Sie eine Spalte aus, nach der gruppiert werden soll.
- **Sortierspaltenrichtung** – `Aufsteigend`, `Absteigend`.
- **Monat** – Wählen Sie einen Monat aus.
- **Jahr** – Wählen Sie ein Jahr aus.
- **Ticket-Volumendiagramm anzeigen** – Wenn aktiviert, wird ein Ticket-Volumendiagramm angezeigt.

Service Desk – Tickets

Info Center > Reporting > Berichte > Service Desk - Tickets

- *Wird nur angezeigt, wenn das Service Desk-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Tickets** wird ein Bericht generiert, in dem Übersichtsinformationen und Details von **Service Desk**-Tickets angezeigt werden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Alle offenen Tickets und solche, die innerhalb der letzten N Tage geschlossen wurden, anzeigen** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Anmerkungen-/Zusammenfassung-/Absenderfilter** – Führt nur Tickets oder Ticketzahlen auf, die diese Zeichenfolge in einer Anmerkung, einer Zusammenfassungs- oder Absenderinformationenzeile enthalten. Verwenden Sie * als Stellvertreterzeichen.
- **Alle Tickets anzeigen** – Wenn aktiviert, werden alle Tickets einzeln aufgeführt.
- **Anmerkungen mit jedem Ticket anzeigen** – Wenn aktiviert, werden mit jedem Ticket Anmerkungen angezeigt.
- **Ausgeblendete Anmerkungen verbergen** – Wenn aktiviert, werden ausgeblendete Anmerkungen verborgen.
- **Sortierspalte** – Wählen Sie die Spalte aus, nach der Tickets sortiert werden sollen.
- **Sortierrichtung** – `Aufsteigend`, `Absteigend`.
- **Ticketstatusdiagramm für jeden Administrator anzeigen** – Zeigt ein separates Ticketstatus-Balkendiagramm für jeden Benutzer und für nicht zugewiesen an.
- **Tortendiagramm für alle Datenspalten der gewählten Ticketkategorie anzeigen** – `Bearbeiter`, `Status`, `Priorität`, `Kategorie`, `Unterkategorie`.

Spaltenfilter

Werte für alle Service Desk-Definitionen werden in den Dropdown-Listen angezeigt. Sie können mit den Tastenkombinationen `Strg + Klicken` und `Umschalt + Klicken` mehrere Elemente auswählen, sofern nicht anderweitig angegeben.

- **Administratorfilter** – Es kann nur jeweils ein Element ausgewählt werden.
- **Statusfilter**
- **Prioritätenfilter**

- **Kategoriefilter**
- **Unterkategorie-Filter** – Es werden nur Unterkategorien für ausgewählte Kategorien im **Kategorie.Filter** angezeigt.

Software – Geänderte Softwareanwendungen

Info Center > Reporting > Berichte > Software - Software-Anwendungen geändert

- Über > Hinzufügen/Entfernen *(siehe 157)* werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Geänderte Softwareanwendungen** wird ein Bericht mit einer Liste der Softwareanwendungen, die zu Rechner-IDs hinzugefügt bzw. von diesen entfernt wurden, generiert. Hierzu werden die bei der letzten Inventarisierung erfassten Daten verwendet.

Hinweis: Vor der Freigabe von Kaseya 2 trug dieser Bericht den Titel **Software – Programme hinzufügen/entfernen**.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Listenelementfilter hinzufügen/entfernen** – Geben Sie eine Zeichenfolge ein, um Elemente nach ihrem Namen zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechner-IDs auflisten, die jede Anwendung beinhalten** – Wenn diese Option aktiviert ist, wird die Rechner-ID jedes Rechners aufgelistet, zu dem ein Programm hinzugefügt bzw. von dem ein Programm entfernt wurde.

Software – Installierte Softwareanwendungen

Info Center > Reporting > Berichte > Software - Software-Anwendungen installiert

- Über Audit > Installierte Anwendungen *(siehe 156)* werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Geänderte Softwareanwendungen** wird ein Bericht generiert, in dem sämtliche auf allen Rechnern gefundenen eindeutigen Anwendungen aufgelistet sind. Außerdem wird die Gesamtanzahl der eindeutigen Kopien der Anwendung aufgelistet. Hierzu werden die bei der letzten Inventarisierung erfassten Daten verwendet.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anwendungsfilter** – Filtert den Bericht nach Anwendungsnamen (App.exe).
- **Produktnamenfilter** – Filtert den Bericht nach der vom Softwareanbieter angegeben Produktnamenzeichenfolge.
- **Beschreibungsfilter** – Filtert den Bericht nach der vom Softwareanbieter angegeben Softwarebeschreibungszeichenfolge.
- **Herstellerfilter** – Filtert den Bericht nach dem Namen des Softwareanbieters.
- **Versionsfilter** – Filtert den Bericht nach der Versionsnummer der Software.
- **Nicht registrierte Anwendungen anzeigen** – Wenn diese Option aktiviert ist, werden auch Programme angezeigt, die nicht in der Registrierung enthalten sind. Registrierte Anwendungen fügen einen `App-Pfad`-Schlüssel in die Registrierung ein, der den Speicherort der primären ausführbaren Datei angibt. Die Sortierung nach diesem Wert ist ein gutes Mittel, die Hauptanwendungen von den Hilfs- und sekundären Anwendungen zu trennen.
- **Rechner-IDs auflisten, die jede Anwendung beinhalten** – Wenn diese Option aktiviert ist, wird die Rechner-ID jedes Rechners aufgelistet, auf dem das aufgelistete Programm installiert ist.
- **Spalte(n) anzeigen** – `Anwendung`, `Produkt`, `Beschreibung`, `Hersteller`, `Version`.
- **Sortieren nach** – `Anwendung`, `Produkt`, `Beschreibung`, `Hersteller`, `Version`.

Software – Softwarelizenzen

Info Center > Reporting > Berichte > Software - Softwarelizenzen

- Über Audit > Softwarelizenzen (siehe 157) werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Softwarelizenzen** wird ein Bericht generiert, in dem sämtliche der in einer Gruppe von Rechnern gefundenen Softwarelizenzen aufgelistet sind. Der Bericht gibt die Gesamtanzahl der Lizenzen sowie die Anzahl der eindeutigen Lizenzen in allen Rechnern an. Hierzu werden die bei der letzten Inventarisierung erfassten Daten verwendet.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Publisher-Matching anzeigen** – Filtert den Bericht nach dem Namen des Softwareanbieters.
- **Titel-Matching anzeigen** – Filtert den Bericht nach Softwaretitel.
- **Rechner-IDs nicht auflisten** – Rechner-IDs werden nicht aufgelistet.
- **Rechner-IDs auflisten** – Die Rechner-IDs aller Rechner, auf denen die Anwendung installiert ist, werden aufgelistet.
- **Rechner-IDs nach Lizenzschlüssel auflisten** – Die auf jedem Rechner installierten Lizenzschlüssel und Produktschlüssel werden aufgelistet.

Software – Softwarelizenzen – Übersicht

Info Center > Reporting > Berichte > Software - Übersicht über Softwarelizenzen

- Über Audit > Softwarelizenzen (siehe 157) werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Softwarelizenzen** wird ein Bericht generiert, in dem die auf allen Rechnern in einer Gruppe oder Ansicht gefundenen Softwarelizenzen übersichtlich dargestellt sind. Hierzu werden die bei der letzten Inventarisierung erfassten Daten verwendet. Dieser Bericht enthält vier Tabellen, in denen die folgenden Informationen zusammengefasst sind:

- **Server** – Listet alle gefundenen Servertypen sowie die Anzahl der Rechner, auf denen dieses Server-Betriebssystem ausgeführt wird, auf.
- **Workstations** – Listet alle gefundenen Workstationtypen sowie die Anzahl der Rechner, auf denen dieses Workstation-Betriebssystem ausgeführt wird, auf.
- **Microsoft Office-Lizenzen** – Listet die Anzahl der Rechner zusammen mit der jeweils geladenen Version von Microsoft Office auf.
- **Andere Anwendungen** – Gibt eine Übersicht über die Anzahl der Rechner, auf denen Anwendungslizenzen gefunden wurden, die nicht in den ersten drei Tabellen enthalten sind.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Publisher-Matching anzeigen** – Filtert den Bericht nach dem Namen des Softwareanbieters.
- **Titel-Matching anzeigen** – Filtert den Bericht nach Softwaretitel.

Software – Betriebssysteme

Info Center > Reporting > Berichte > Software - Betriebssysteme

Mit der Berichtsdefinition **Betriebssysteme** wird ein zusammengesetztes Diagramm sämtlicher auf allen Rechner-IDs gefundenen Betriebssysteme generiert.

> **Hinweis:** Für jeden Rechner werden Typ und Version des Betriebssystems bei jedem Check-in angezeigt. Zur Erfassung von Informationen zum Betriebssystem muss das Audit nicht unbedingt abgeschlossen sein. Es ist daher möglich, dass die von diesem Bericht gemeldete Anzahl der Betriebssystem höher als die für dieses Betriebssystem angegebene Anzahl der Lizenzen ist, falls noch nicht für alle Rechner eine Inventarisierung abgeschlossen wurde.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- Tortendiagramm anzeigen
- Balkendiagramm anzeigen
- Tabelle anzeigen

Softwarebereitstellung – Profilstatus nach Rechner

Info Center > Reporting > Berichte > Softwarebereitstellung - Profilstatus nach Rechner

- Wird nur angezeigt, wenn das Software Deployment and Update-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Profilstatus nach Rechner** wird ein Bericht generiert, in dem der Compliance-Status von durch **Software Deployment and Update** verwalteten Rechnern aufgeführt ist.

- **Optionen anzeigen** – `Detailliert` oder `Übersicht`

Softwarebereitstellung – Aktuelle Bereitstellungen

Info Center > Reporting > Berichte > Softwarebereitstellung - Aktuelle Bereitstellungen

- Wird nur angezeigt, wenn das Software Deployment and Update-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Aktuelle Bereitstellungen** wird ein Bericht generiert, in dem die neuesten Bereitstellungen aufgeführt sind.

Zeitrahmen

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Softwarebereitstellung – Software von Rechner installiert

Info Center > Reporting > Berichte > Softwarebereitstellung - Software von Rechner installiert

- Wird nur angezeigt, wenn das Software Deployment and Update-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Software von Rechner installiert** wird ein Bericht mit einer Liste der Softwaretitel generiert, die auf durch **Software Deployment and Update** verwalteten Rechnern installiert sind.

- **Optionen anzeigen** – `Detailliert` oder `Übersicht`

Softwarebereitstellung – Änderungen an Rechnern

Info Center > Reporting > Berichte > Softwarebereitstellung - Aktuelle Bereitstellungen

- Wird nur angezeigt, wenn das Software Deployment and Update-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Änderungen an Rechnern** wird ein Bericht generiert, in dem die Softwaretitel und die Versionsänderungen auf durch **Software Deployment and Update** verwalteten Rechnern aufgeführt sind.

Vergleichsparameter

- **Mit Basis-Scan des Rechners vergleichen** – Durch einen Vergleich der Informationen aus dem aktuellen Scan mit denen aus dem Referenzscan werden sämtliche Softwareänderungen angezeigt, die auf jedem Rechner ermittelt wurden.

- **Mit ausgewählter Rechner-ID vergleichen** – Durch einen Vergleich der Informationen aus dem aktuellen Scan mit denen aus dem Scan einer *ausgewählten Rechner-ID* werden sämtliche Softwareänderungen angezeigt, die auf jedem Rechner ermittelt wurden. Anhand dieser Funktion können Sie Unterschiede in einer Gruppe von Rechnern im Vergleich zu den Standardangaben für die Gruppe identifizieren.
- **Grundwert-Scan verwenden** – Aktiviert, wenn **Mit ausgewählter Rechner-ID vergleichen** ausgewählt ist. Wenn diese Option aktiviert ist, wird der Referenzscan der ausgewählten Rechner-ID anstelle des aktuellen Scans für den Vergleich herangezogen.

Optionen anzeigen

- **Aktualisierungen anzeigen** – Rechner, deren Software aktualisiert wurde.
- **Hinzugefügtes anzeigen** – Rechner, auf denen zusätzliche Software installiert wurde.
- **Entfernungen anzeigen** – Rechner, auf denen Software deinstalliert wurde.
- **Keine Änderungen anzeigen** – Rechner, an denen keine Softwareänderungen vorgenommen wurden.
- **"Ohne-Profil" anzeigen** – Rechner, auf denen keine Profile zugeordnet wurden.

Ticketing – Anpassbares Ticketing

Info Center > Reporting > Berichte > Ticketing > Anpassbares Ticketing

- Über Ticketing > Übersicht anzeigen *(siehe 457)* werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Anpassbares Ticketing** wird ein Bericht generiert, in dem alle Tickets des **Ticketing**-Moduls, die ausgewählten Organisationen, Rechnergruppen, Rechnern, Abteilungen oder Mitarbeiterdatensätzen zugewiesen sind, angezeigt werden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Bestimmter Zeitbereichstyp** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Alle offenen Tickets und solche, die innerhalb der letzten N Tage geschlossen wurden, anzeigen** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Ticketstatusdiagramm für jeden Administrator anzeigen** – Zeigt ein separates Ticketstatus-Balkendiagramm für jeden Benutzer und für nicht zugewiesen an.
- **Tortendiagramm für jede gewählte Ticketkategorie anzeigen** – `Bearbeiter`, `Status`, `Kategorie`, `Priorität`.
- **Keine anzeigen** – Es werden keine einzelnen Tickets im Bericht aufgeführt.
- **Alle Tickets anzeigen** – Alle Tickets werden einzeln aufgeführt.
- **Alle Tickets mit Anmerkungen anzeigen** – Alle Tickets, einschließlich öffentlicher und ausgeblendeter Anmerkungen werden aufgeführt.
- **Alle Tickets anzeigen, jedoch ausgeblendete Anmerkungen verbergen** – Alle Tickets, einschließlich öffentlicher Anmerkungen werden aufgeführt, ausgeblendete Anmerkungen werden jedoch verborgen.

Filter

- **Anmerkungen-/Zusammenfassung-/Absenderfilter** – Geben Sie eine Zeichenfolge ein, um Tickets nach ihrer Anmerkungen- oder Filterzeile und nach den Absenderfeldern zu filtern. Schließend Sie ein

Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.

- **Bearbeiter-Filter** – Filtern Sie Tickets nach Bearbeiter.
- **Sortierspalte** – Wählen Sie die Spalte aus, nach der Tickets sortiert werden sollen.
- **Sortierrichtung** – `Aufsteigend`, `Absteigend`.
- **Status** – Filtern Sie Tickets nach Status.
- **Kategorie** – Filtern Sie Tickets nach Kategorie.
- **Priorität** – Filtern Sie Tickets nach Priorität.
- **Lösung** – Filtern Sie Tickets nach Lösung.
- **(Benutzerdefinierte Felder)** – Filtern Sie Tickets nach einem oder mehreren benutzerdefinierten Feld(ern).

Spalten

Wählen Sie die im Bericht enthaltenen Ticketspalten. Alle Spalten sind standardmäßig enthalten.

Ticketing – Ticketing

Info Center > Reporting > Berichte > Ticketing > Ticketing

- Über Ticketing > Übersicht anzeigen *(siehe 457)* werden ähnliche Informationen bereitgestellt.

Mit der Berichtsdefinition **Ticketing** wird ein Bericht generiert, in dem alle Tickets des **Ticketing**-Moduls, die ausgewählten Organisationen, Rechnergruppen, Rechnern, Abteilungen oder Mitarbeiterdatensätzen zugewiesen sind, angezeigt werden.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Alle offenen Tickets und solche, die innerhalb der letzten N Tage geschlossen wurden, anzeigen** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Ticketstatusdiagramm für jeden Administrator anzeigen** – Zeigt ein separates Ticketstatus-Balkendiagramm für jeden Benutzer und für nicht zugewiesen an.
- **Tortendiagramm für jede gewählte Ticketkategorie anzeigen** – `Bearbeiter`, `Status`, `Kategorie`, `Priorität`.
- **Anmerkungen-/Zusammenfassung-/Absenderfilter** – Führt nur Tickets oder Ticketzahlen auf, die diese Zeichenfolge in einer Anmerkung, einer Zusammenfassungs- oder Absenderinformationenzeile enthalten. Verwenden Sie * als Stellvertreterzeichen.
- **Keine anzeigen** – Es werden keine einzelnen Tickets im Bericht aufgeführt.
- **Alle Tickets anzeigen** – Alle Tickets werden einzeln aufgeführt.
- **Alle Tickets mit Anmerkungen anzeigen** – Alle Tickets, einschließlich öffentlicher und ausgeblendeter Anmerkungen werden aufgeführt.
- **Alle Tickets anzeigen, jedoch ausgeblendete Anmerkungen verbergen** – Alle Tickets, einschließlich öffentlicher Anmerkungen werden aufgeführt, ausgeblendete Anmerkungen werden jedoch verborgen.
- **Anmerkungen-/Zusammenfassung-/Absenderfilter** – Geben Sie eine Zeichenfolge ein, um Tickets nach ihrer Anmerkungen- oder Filterzeile und nach den Absenderfeldern zu filtern. Schließend Sie ein

Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.

- Tickets filtern nach
  - **Bearbeiter**
  - **Status**
  - **Kategorie**
  - **Priorität**
- **Sortierspalte** – Wählen Sie die Spalte aus, nach der Tickets sortiert werden sollen.
- **Sortierrichtung** – `Aufsteigend`, `Absteigend`.

Zeitverfolgung – Arbeitszeittabellen-Übersicht

Info Center > Reporting > Berichte > Zeitverfolgung > Arbeitszeittabellen-Übersicht

Mit der Berichtsdefinition **Arbeitszeittabellen-Übersicht** wird ein Bericht generiert, in dem der Status aller Arbeitszeittabellen für einen angegebenen Datumsbereich aufgeführt ist.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Benutzerdefinierte(s) Startdatum/-zeit** – Das Startdatum.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Das Enddatum.

Parameter

- **Gruppentyp auswählen** – Gruppiert nach `Periode` oder nach `Status`.
- **Personalliste** – Die in den Bericht aufzunehmenden Mitarbeiter. In der Liste werden alle Mitarbeiter mit Arbeitszeittabellen aufgeführt, für die Sie die Ihrem Scope entsprechende Anzeigeberechtigung besitzen.

> **Hinweis:** Für jeden Personaldatensatz und Zeitraum wird ein Zeiterfassungsbeleg nur erstellt, wenn zumindest ein Zeiteintrag in diesen Zeiterfassungsbeleg eingefügt wird.

Zeitverfolgung – Einträge in Arbeitszeittabelle

Info Center > Reporting > Berichte > Zeitverfolgung > Einträge in Arbeitszeittabelle

Mit der Berichtsdefinition **Einträge in Arbeitszeittabelle** wird ein Bericht generiert, in dem alle Arbeitszeittabellen-Einträge für einen angegebenen Datumsbereich aufgeführt sind.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Benutzerdefinierte(s) Startdatum/-zeit** – Das Startdatum.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Das Enddatum.

Parameter

- **Personalliste** – Die in den Bericht aufzunehmenden Mitarbeiter. In der Liste werden alle Mitarbeiter mit Arbeitszeittabellen aufgeführt, für die Sie die Ihrem Scope entsprechende Anzeigeberechtigung besitzen.

Verwaltungs-Dashboard

Info Center >Dashboard > Verwaltungs-Dashboard

Auf der Seite **Verwaltungs-Dashboard** wird der aktuelle Status aller Agent-Rechner angezeigt, für die ein VSA-Benutzer Anzeigerechte besitzt. Das Dashboard setzt sich aus einem Set von Dashlets zusammen, wobei jedes Dashlet eine spezielle Metrik anzeigt.

- Alle Agent-Dashlets bieten die Möglichkeit zur Detailanzeige, sodass eine Liste der einzelnen Agent-Rechner in diesem Dashlet angezeigt werden kann.
- Dashboards können nach Scope und **Rechner-ID/Gruppen-ID** *(siehe 26)* gefiltert werden.

Zu den auf dieser Seite angezeigten Dashlets zählen:

- **Rechner online**
- **Server online**
- **Server offline**
- **Agents mit anstehendem Neustart**
- **Agents, denen Patches mit einer Patch-Richtlinie fehlen**
- **Agents, die Richtlinien nicht mehr erfüllen** und denen **Policy Management**-Richtlinien zugeordnet sind.
- **Agents ohne Richtlinien**, die durch **Policy Management** zugewiesen wurden.
- **Ausgesetzte Agents**
- **Rechner mit geringem Speicherplatz**
- **Agents in einer unbenannten Gruppe**
- **Agents, denen Patches ohne eine Patch-Richtlinie fehlen**
- **Der ersten zehn Rechner mit geringem Speicherplatz**
- **Agent-Verfahren mit ausstehender Genehmigung**
- **Eingeloggte Administratoren**

Aktionen

- Klicken Sie auf ein beliebiges Dashlet, um eine Liste der einzelnen Rechner und Geräte in diesem Dashlet anzuzeigen.

Dashboard anzeigen

Info Center > Dashboard > Dashboard anzeigen>

Auf der Seite **Dashboard anzeigen** erhalten Sie einen kurzen Überblick über den Status des gesamten Systems, wobei die Rechner-IDs und die Aufgaben, die Sie als erstes ausführen müssen, hervorgehoben werden. Die vom Dashboard angezeigten Ergebnisse sind vom **Rechner-ID-/Gruppen-ID-Filter** *(siehe 626)* abhängig. Sie können **Aufgaben** verwalten und **Nachrichten** an andere Benutzer über das Dashboard senden. Mit Info Center > **Dashboard gestalten** *(siehe 243)* können Sie die Dashboard-Anzeige anpassen.

Agentstatus

Über diese Option erhalten Sie eine Übersicht des Online-Status aller Rechner-IDs, die den aktuellen Rechner-ID-/Gruppen-ID-Filter erfüllen. Sie erhalten eine klare Vorstellung davon, wie viele Rechner **online** sind, bei wie vielen **Benutzer angemeldet** sind, seit **weniger als 30 Tagen** bzw. seit **mehr als 30 Tagen** offline sind, sowie die **Gesamtanzahl der Agents**, die den aktuellen Rechner-ID-/Gruppen-ID-Filter erfüllen.

Patch-Status

Mit dieser Option werden anhand eines Kreisdiagramms alle Rechner hervorgehoben, auf denen Patches fehlen und die den aktuellen Rechner-ID-/Gruppen-ID-Filter erfüllen. Das Diagramm wird angezeigt, unabhängig davon, ob Sie eine Patch-Regeln anwenden oder nicht.

- Klicken Sie auf **Richtlinie verwenden**, um beim Generieren des Kreisdiagramms die **Patch-Richtlinie** *(siehe 624)* anzuwenden.

> **Hinweis:** Beim Anwenden der Patch-Richtlinie ist mit erheblichen Leistungseinbußen zu rechnen. Falls Sie sehr viele Rechner-IDs haben, kann das Generieren des Kreisdiagramms sehr lang dauern, wenn Sie die Patch-Richtlinie verwenden.

- Klicken Sie auf **Richtlinie ausblenden**, um das Kreisdiagramm ohne Verwendung der Patch-Richtlinie zu generieren. Dadurch werden alle fehlenden Patches aufgezeigt, einschließlich derjenigen, die von der Patch-Richtlinie abgelehnt wurden.
- Beim Klicken auf ein beliebiges Kreissegment wird ein Teilfenster geöffnet, in dem alle Rechner-IDs aufgelistet werden, aus denen sich dieses Kreissegment zusammensetzt.

Betriebssysteme

Verwendet ein Kreisdiagramm, um die Kombination der verwendeten Betriebssysteme für Rechner zu zeigen, die den aktuellen Rechner-ID-/Gruppen-ID-Filter erfüllen. Beim Klicken auf ein beliebiges Kreissegment wird ein Teilfenster geöffnet, in dem alle Rechner-IDs aufgelistet werden, aus denen sich dieses Kreissegment zusammensetzt.

Tickets

Hiermit werden die kürzlich ausgestellten Tickets für alle Rechner-IDs aufgelistet, die den aktuellen Rechner-ID-/Gruppen-ID-Filter erfüllen. Diese Einstellung gilt nur für Tickets, die mit dem **Ticketing**-Modul ausgestellt wurden.

Systemstatus

Identifiziert die Anzahl der aktuellen VSA-Benutzer und **Portalzugriff** *(siehe 75)*-Benutzer und deren Anzahl insgesamt. Außerdem werden die Größe der Datenbank, die Datenbankgröße pro Rechnerkonto sowie das letzte Sicherungsdatum angezeigt.

Aufgaben

In diesem Abschnitt können Sie Aufgaben erstellen, bearbeiten und überwachen, die Sie oder andere Benutzer ausführen müssen. In einem Popup-Fenster werden Sie darauf hingewiesen, wenn neue Aufgaben, die für Sie erstellt wurden, zu Ihrer Aufgabenliste hinzugefügt wurden. Wenn eine Aufgabe überfällig wird, werden möglicherweise weitere Popups eingeblendet. Sie können das System anweisen, Sie erneut an ein Fälligkeitsdatum zu erinnern, indem Sie beim Einblenden des Dialogfelds zur Aufgabenerinnerung auf die Schaltfläche **Sparmodus** klicken. Sie können alle ausstehenden Aufgabenbenachrichtigungen löschen, indem Sie auf die Schaltfläche **Sparmodus löschen** auf der Seite System > **Voreinstellungen** *(siehe 402)* klicken.

Meldungen

In diesem Abschnitt können Sie Nachrichten an andere VSA-Benutzer senden. Andere VSA-Benutzer sehen diese Nachrichten als Popup-Fenster. Nachrichten, die Sie erhalten haben, werden im unteren Bereich dieses Fensters aufgelistet.

> **Hinweis:** Nachrichten an Rechnerbenutzer werden über Fernsteuerung > **Nachricht senden** *(siehe 391)* gesendet.

Layout-Dashboard

Info Center > Dashboard > Layout

Auf der Seite **Layout-Dashboard** werden die einzelnen Bereiche der Seite **Dashboard anzeigen** *(siehe 241)* angezeigt bzw. ausgeblendet und ihre Reihenfolge von oben nach unten festgelegt. Um ein Element anzuzeigen, aktivieren Sie das Kontrollkästchen neben dem Element.

Für zwei Elemente stehen weitere Anpassungsoptionen zur Verfügung: **Tickets** und **Nachrichten**. Beide zeigen zeitabhängige Daten an. Damit neue Elemente leichter von älteren Elementen unterschieden werden können, können Sie abhängig davon, wann das Datenelement generiert wurde, verschiedene Markierungsfarben aus Datenzeilen auswählen.

Empfehlung

- Markieren Sie die neuesten Tickets und Nachrichten in rot. Alle Tickets und Nachrichten, die in den letzten N Tagen erstellt wurden, werden rot markiert.
- Markieren Sie die neuesten Tickets und Nachrichten in gelb. Alle Tickets und Nachrichten, die älter als das rot markierte Datum, jedoch neuer als die eingegeben Zahl sind, werden gelb markiert.
- Deaktivieren Sie die Markierung, indem Sie die Anzahl Tage auf Null setzen.

Kapitel 7

Monitor

In diesem Kapitel

Monitor – Übersicht

Monitor

Das **Monitoring**-Modul in **Virtual System Administrator™** stellt sechs Monitoring-Methoden von Rechnern und Protokolldateien zur Verfügung:

- **Meldungen** – Überwacht Ereignisse auf *Agent*-Rechnern.
- **Ereignisprotokoll-Meldungen** – Überwacht Ereignisse in den Ereignisprotokollen der *Agent*-Rechner.
- **Monitor-Sets** – Überwacht den Leistungsstatus auf *Agent*-Rechnern.
- **SNMP-Sets** – Überwachen den Leistungsstatus auf *Geräten ohne Agent*.
- **Systemprüfung** – Überwacht Ereignisse auf *Rechnern ohne Agent*.
- **Protokoll-Monitoring** – Überwacht Ereignisse in *Protokolldateien*.

Sie können den Systemzustand von verwalteten Rechnern und SNMP-Geräten in Echtzeit überwachen und sofort benachrichtigt werden, wenn irgendwelche Probleme auftreten. Wenn programmierbare Alarme ausgelöst werden, werden über **Monitor** E-Mail-Benachrichtigungen, Verfahren und Job-Tickets veranlasst. Hierzu zählen Probleme und Statusänderungen wie die folgenden:

- Wenn kritische Server oder Arbeitsplatzcomputer offline gehen.
- Wenn ein Benutzer die Fernsteuerung deaktiviert.
- Wenn eine Softwareanwendung hinzugefügt oder entfernt wird.
- Wenn sich die Hardwarekonfiguration ändert.
- Wenn der Computer fast keinen Speicherplatz mehr hat.
- Wenn ein Protokolleintrag zu einem bestimmten oder beliebigen Ereignis erzeugt wird.
- Wenn eine Schutzregelverletzung auftritt.
- Wenn ein Agent-Verfahren nicht ausgeführt wird.
- Wenn eine nicht zugelassene Anwendung versucht, auf das Netzwerk zuzugreifen.
- Wenn eine nicht zugelassene Anwendung versucht, auf eine geschützte Datei zuzugreifen.
- Wenn ein neues Gerät im LAN erscheint.
- Wenn in einem externen Protokoll ein bestimmter Protokolleintrag aufgezeichnet wird.

Zusätzlich zur Generierung von Meldungsbenachrichtigungen, wenn **Ereignisprotokolleinträge** erstellt werden, werden die von Ihren verwalteten Rechner gesammelten Ereignisprotokolleinträge auf dem VSA gespeichert Die Ereignisprotokolldaten sind immer verfügbar, selbst wenn der verwaltete Rechner offline oder ausgefallen ist. Ereignisprotokolldaten werden in einer bekannten und präzisen Form auf der Seite Agent > **Agent-Protokolle** *(siehe 35)* sowie unter Info Center > Reporting > Berichte > Protokolle angezeigt.

Hinweis: Unter dem ersten Thema der Online-Hilfe können Sie die PDF-Datei **Kontrollkonfiguration** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_monitoringconfiguration70.pdf#zoom=70&navpanes=0)* herunterladen.

Hinweis: Unter dem ersten Thema der Online-Hilfe können Sie die PDF-Datei **Schrittweise Konfiguration von Protokollanalysen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_logparsers70.pdf#zoom=70&navpanes=0)* herunterladen.

Hinweis: Mit **Kaseya Monitor™ Service** (**http://www.kaseya.com/services/it-services.aspx**) wird das Monitoring über die normalen Bürozeiten hinaus erweitert. Indem die Systemverwaltung und das Monitoring auf Zeiten außerhalb des Bürobetriebs verlegt werden, können MSPs Kunden ein ununterbrochenes Monitoring rund um die Uhr anbieten.

Hinweis: Jeder Agent, der zur Überwachung verwendet wird, muss über die Seite Agent > **Agent aktualisieren** *(siehe 81)* aktualisiert werden.

Funktion	Beschreibung
Dashboardliste *(siehe 251)*	Stellt mehrere Kontrollansichten zur Verfügung.
Dashboard-Einstellungen *(siehe 260)*	Benutzer können die Dashboard-Liste nach Belieben anpassen.
Alarmübersicht *(siehe 260)*	Listet die Alarme für überwachte Rechner auf.
Alarme unterbrechen *(siehe 262)*	Setzt die Alarmbenachrichtigungen für bestimmte Rechner-IDs aus.
Live Counter *(siehe 263)*	Zeigt Live-Leistungszählerdaten für die ausgewählte Rechner-ID an.
Monitorlisten *(siehe 264)*	Konfiguriert die Monitorlistenobjekte für das Monitoring.
Listen durch Scan aktualisieren *(siehe 266)*	Scannt Rechner auf Kontrollzähler und Dienste.
Monitor-Sets *(siehe 267)*	Konfiguriert Monitor-Sets.
SNMP-Sets *(siehe 276)*	Konfiguriert SNMP-Monitor-Sets.
SNMP-Objekt hinzufügen *(siehe 281)*	Verwaltet SNMP MIB-Objekte.
Meldungen *(siehe 284)*	Konfiguriert Monitor-Meldungen für Rechner.
Ereignisprotokoll-Meldungen *(siehe 316)*	Löst eine Meldung für einen Ereignisprotokolleintrag aus.
SNMP-Traps-Meldung *(siehe 323)*	Konfiguriert Meldungen für SNMP-Trap-Ereignisprotokolleinträge, die auf ausgewählten verwalteten Rechnern erstellt wurden.
Monitoring zuweisen *(siehe 327)*	Weist Alarme von Monitor-Sets auf Rechnern zu, entfernt und verwaltet sie.
Monitor-Protokoll *(siehe 333)*	Zeigt Monitor-Protokolldaten im Diagramm- und Tabellenformat an.
Systemprüfung *(siehe 336)*	Weist Alarme für Systemprüfungen auf Rechnern zu, entfernt und verwaltet sie.
SNMP zuordnen *(siehe 340)*	Weist Alarme von SNMP-Monitor-Sets auf Geräten zu, entfernt und verwaltet sie.
SNMP-Protokoll *(siehe 349)*	Zeigt SNMP-Protokolldaten im Diagramm- und Tabellenformat an.
SNMP-Werte einrichten *(siehe 350)*	Legt die SNMP-Werte auf dem angegebenen Gerät fest.
SNMP-Typ konfigurieren *(siehe 352)*	Weist SNMP-Typen den SNMP-Geräten zu.
Parser-Übersicht *(siehe 353)*	Definiert Alarme für Analysesätze und kopiert die Analysesatzzuweisungen auf mehrere Rechner-IDs.
Log-Parser *(siehe 357)*	Definiert Protokollanalysen und weist sie Rechner-IDs zu.
Parser-Sets zuweisen *(siehe 363)*	Erstellt Analysesätze und weist sie Rechner-IDs zu und erstellt Meldungen für Analysesatzzuweisungen.

Kontrollbedingungen und -konzepte

Für alle Monitoring-Methoden gelten die gleichen Meldungsverwaltungsbedingungen und -konzepte.

Meldungen und Alarme

- **Meldungen** – Eine Meldung wird erstellt, wenn die Leistung eines Rechners oder Geräts mit einem vordefinierten Kriterium oder einer „Meldungsbedingung“ übereinstimmt.
- **Alarme** – *Alarme* sind eine grafische Methode, um den Benutzer zu benachrichten, dass ein *Alarm* aufgetreten ist. In vielen grafischen Anzeigen im VSA wird im Falle einer Meldung standardmäßig im VSA ein rotes Ampelsymbol angezeigt. Liegt kein Alarm vor, wird ein grünes Ampelsymbol angezeigt. Diese Symbole können angepasst werden.
- **Protokolle** – Zwei Protokolle unterscheiden zwischen Meldungen und Alarmen.
  - **Alarmprotokoll** – Verfolgt sämtliche *Alarme, die von einer Meldung erstellt wurden.*
  - **Monitor-Aktionsprotokoll** – Verfolgt sämtliche *erstellten Meldungen*, unabhängig davon, ob ein Alarm oder ein anderer Aktionstyp als Reaktion auf die Meldung ergriffen wurde.

Aktionen

Erstellen eines Alarms ist nur ein *Aktionstyp*, der ergriffen werden kann, wenn eine Meldung auftritt. Die anderen Aktionstypen sind Benachrichtigungen. Diese umfassen **das Senden einer E-Mail** oder **Erstellen eines Tickets**. Ein vierter Aktionstyp ist das **Ausführen eines Agent-Verfahrens**, um automatisch auf die Meldung zu reagieren. Diese vier Arten von Aktionen werden als **ATSE-Code** bezeichnet. Der ATSE-Code gibt an, welche Arten von Aktionen für die definierte Meldung aktiv sind, unabhängig davon, ob sie einer Rechner-ID, einer Gruppen-ID oder einem SNMP-Gerät zugewiesen sind.

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

Keine der ATSE-Aktionen wird benötigt. Die Meldung und die ATSE-Aktion (einschließlich keine Aktion) werden im Bericht Info Center > Monitor – **Monitor-Aktionsprotokoll** *(siehe 224)* ausgegeben.

Meldungstypen

Zu den Arten von Meldungen gehören:

- Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*
- Sicherung > Sicherungsmeldungen
- Monitor > **Meldungen** *(siehe 284)* – Dies sind spezielle „festgelegte“ Meldungen, die sofort auf einen Rechner angewendet werden können.
- Monitor > **Monitor zuweisen** *(siehe 327)*
- Monitor > **SNMP-Traps-Meldung** *(siehe 323)*
- Monitor > **SNMP zuweisen** *(siehe 340)*
- Monitor > **Systemprüfungen** *(siehe 336)*
- Monitor > **Analyse-Übersicht** *(siehe 353)*
- Monitor > **Analysesätze zuweisen** *(siehe 363)*
- Patch-Management > Patch-Meldungen
- Fernsteuerung > Externe Meldungen
- Sicherheit > Alarmsätze anwenden

Andere Zusatzmodule verfügen über Meldungen, die hier nicht aufgelistet sind.

Sechs Monitoring-Methoden

Jede der sechs Monitoring-Methoden in **Virtual System Administrator™** ist entweder *ereignisbasiert*

oder *statusbasiert*.

- Ereignisbasiert
  - **Meldungen** – Überwacht Ereignisse auf *Agent*-Rechnern.
  - **Ereignisprotokoll-Meldungen** – Überwacht Ereignisse in den Ereignisprotokollen der *Agent*-Rechner
  - **Systemprüfung** – Überwacht Ereignisse auf Rechnern *ohne Agent*
  - **Protokoll-Monitoring** – Überwacht Ereignisse in *Protokolldateien*.
- Statusbasiert
  - **Monitor-Sets** – Überwacht den Leistungsstatus auf *Agent*-Rechnern
  - **SNMP-Sets** – Überwachen den Leistungsstatus auf *Geräten ohne Agent*

Ereignisbasierte Meldungen

Meldungen *(siehe 284)*, **Systemprüfung** *(siehe 336)*, Ereignisprotokoll-Meldungen und **Protokoll-Monitoring** *(siehe 357)* stellen **ereignisbasierte Meldungen** dar, die nur vereinzelt auftreten. So kann beispielsweise eine Sicherung fehlschlagen. Auch wenn die Sicherung später erfolgreich ist, ist das Fehlschlagen ein historisches Ereignis im Alarmprotokoll. Wird ein Alarm für diesen Ereignistyp erstellt, *bleibt der Alarm im Alarmprotokoll „offen", selbst wenn die Meldungsbedingung wiederhergestellt ist.* Sie verwenden in der Regel die Seite **Alarmübersicht** *(siehe 260)*, um Alarme zu überprüfen, die von ereignisbasierten Meldungen erstellt wurden. Wurde das Problem gelöst, „schließen" Sie den Alarm.

Ereignisbasierte Meldungen sind für gewöhnlich leichter zu konfigurieren, da die einzigen Möglichkeiten darin bestehen, ob ein oder mehrere Ereignis(se) innerhalb einer vorgegebenen Zeitspanne eingetreten sind oder nicht.

Statusbasierte Meldungen

Monitor-Set *(siehe 267)*-Zähler, -Dienste und -Prozesse sowie **SNMP-Set** *(siehe 276)*-Objekte liegen gegenwärtig entweder innerhalb ihres erwarteten Statusbereichs oder außerhalb dieses Bereichs, worauf *dynamisch* durch grüne oder rote Alarmsymbole in Dashlet-Überwachungen hingewiesen wird. Diese werden als **statusbasierte Meldungen** bezeichnet.

- *Falls gegenwärtig eine Meldungsbedingung vorliegt, wird in Monitor-Dashlets (siehe 251) ein rotes Alarmsymbol angezeigt.*
- *Falls gegenwärtig keine Meldungsbedingung vorliegt, wird in Kontroll-Dashlets ein grünes Alarmsymbol angezeigt.*

Wenn Sie einen Alarm für statusbasierte Meldungen erstellen, werden Alarmeinträge im Alarmprotokoll erstellt, die den ereignisbasierten Alarmen entsprechen. Diese können dann geschlossen werden. Da statusbasierte Meldungen jedoch in der Regel dynamisch in eine Meldungsbedingung ein- und aus dieser austreten, empfiehlt es sich, nicht jedes Mal, wenn dies geschieht, einen Alarm zu erstellen. Verwenden Sie stattdessen das Dashlet **Netzwerkstatus** *(siehe 255)*, um den *aktuellen Status* der statusbasierten Meldungen zu identifizieren. Sobald das Problem auf dem Rechner oder Gerät behoben wurde, wechselt der Meldungsstatus automatisch auf ein grünes Symbol zurück. Sie müssen die Meldung in diesem Dashlet nicht manuell „schließen".

> **Hinweis:** Wenn Sie herkömmliche Alarme speziell für Monitor-Sets und Offline-Meldungen erstellen, können diese beiden Meldungstypen bei Wiederherstellung geschlossen werden. Weitere Informationen erhalten Sie im Kontrollkästchen **Autom. Schließen für Alarme und Tickets aktivieren** auf der Seite System > **Konfigurieren** *(siehe 429)*.

Die Konfiguration von statusbasierten Alarmen erfordert in der Regel etwas mehr Überlegung als die von ereignisbasierten Alarmen, da mit diesen der Grad der Leistung gemessen wird und nicht nur ein einfaches Versagen.

Dashboards und Dashlets

Die Seite **Dashboard-Liste** ist die primäre Oberfläche des VSA, um Kontrolldaten, einschließlich

Meldungen und Alarme, anzuzeigen. Über die Seite **Dashboard-Liste** werden konfigurierbare Kontrollfenster namens **Dashboard-Ansichten** gepflegt. Jedes Dashboard enthält einen oder mehrere Fensterbereiche mit Kontrolldaten, die als **Dashlets** bezeichnet werden. Jeder VSA-Benutzer kann seine eigenen angepassten Dashboards erstellen. Zu den Arten von Dashlets gehören:

- **Alarmliste** *(siehe 253)*
- **Alarm-Netzwerkstatus** *(siehe 253)*
- **Alarm Rotator** *(siehe 255)*
- **Alarm Ticker** *(siehe 255)*
- **Netzwerkstatus** *(siehe 255)*
- **Gruppenalarmstatus** *(siehe 256)*
- **Monitor-Set-Status** *(siehe 256)*
- **Monitorstatus** *(siehe 259)*
- **Rechner online** *(siehe 259)*
- **Top N – Monitoralarmliste** *(siehe 259)*

Überprüfen von Alarmen

Alle Meldungsbedingungen, für die das Kontrollkästchen **Alarm erstellen** aktiviert ist – sowohl status- als auch ereignisbasierte Alarme – werden im **Alarmprotokoll** aufgezeichnet. Ein im Alarmprotokoll aufgeführter Alarm weist nicht unbedingt auf den *aktuellen Status* eines Rechners oder Geräts hin, sondern ist vielmehr eine *Aufzeichnung* eines Alarms, der *in der Vergangenheit* aufgetreten ist. Ein Alarmprotokoll-Datensatz bleibt solange `Open`, bis Sie ihn schließen.

Erstellte Alarme können geprüft, `geschlossen` oder **gelöscht...** werden. Verwenden Sie hierzu die folgenden Optionen:

- Monitor > **Alarm-Übersicht** *(siehe 260)*
- Monitor > Dashboard-Liste > beliebiges **Alarm-Übersichtsfenster** *(siehe 253)* in einem Dashlet
- Agent > Agent-Protokolle > **Alarmprotokoll** *(siehe 35)*
- **Live Connect** *(siehe 393)* > Agent-Daten > Agent-Protokolle > Alarmprotokoll

Erstellte Alarme können auch mit folgenden Optionen geprüft werden:

- Monitor > Dashboard-Liste > **Alarmliste** *(siehe 253)*
- Monitor > Dashboard-Liste > **Alarm-Netzwerkstatus** *(siehe 253)*
- Monitor > Dashboard-Liste > **Alarm Rotator** *(siehe 255)*
- Monitor > Dashboard-Liste > **Alarm Ticker** *(siehe 255)*
- Monitor > Dashboard-Liste > **Gruppenalarmstatus** *(siehe 255)*
- Monitor > Dashboard-Liste > **Monitor-Set-Status** *(siehe 256)*
- Monitor > Dashboard-Liste > **Monitorstatus** *(siehe 259)*
- Monitor > Dashboard-Liste > **Top N – Anzahl der Monitoralarme** *(siehe 259)*
- Monitor > Dashboard-Liste > **KES-Status** *(siehe 259)*
- Monitor > Dashboard-Liste > **KES-Bedrohungen** *(siehe 260)*
- Info Center > Reporting > Berichte > Monitoring > Protokolle > Alarmprotokoll
- Info Center > Reporting > Berichte > Monitoring > Monitor-Aktionsprotokoll

Prüfen der Leistung (mit oder ohne Erstellen von Alarmen)

Sie können den *aktuellen Status* der Leistungsergebnisse von Monitor-Sets und SNMP-Sets *mit oder ohne Erstellen von Alarmen* prüfen. Verwenden Sie hierfür folgende Optionen:

- Monitor > **Live Counter** *(siehe 263)*
- Monitor > **Monitor-Protokoll** *(siehe 333)*
- Monitor > **SNMP-Protokoll** *(siehe 349)*
- Monitor > Dashboard > **Netzwerkstatus** *(siehe 255)*
- Monitor > Dashboard > **Gruppenalarmstatus** *(siehe 256)*

- Monitor > Dashboard > **Monitor-Set-Status** *(siehe 256)*
- Info Center > **Reporting** *(siehe 164)* > Berichte > Monitoring > Protokolle

Alarme aussetzen

Das Auslösen von Alarmen kann ausgesetzt werden. Über die Seite **Alarme aussetzen** können Sie **Alarme** *(siehe 622)* für vorgegebene Zeitspannen, einschließlich wiederkehrender Zeitperioden, aussetzen. Dadurch können Sie Aufrüstungs- und Pflegeaufgaben durchführen, ohne einen Alarm auszulösen. Wenn Alarme für eine Rechner-ID ausgesetzt sind, *sammelt der Agent weiterhin Daten, generiert jedoch keine zugehörigen Alarme*.

Gruppenalarme

Alarme für Meldungen, Ereignisprotokoll-Meldungen, Systemprüfung und Protokoll-Monitoring werden automatisch einer **Gruppenalarm**-Kategorie zugewiesen. Beim Auslösen eines Alarms wird auch der zugehörige Gruppenalarm ausgelöst. Die Gruppenalarm-Kategorien für Monitor-Sets und SNMP-Sets werden bei der Definition der Sets manuell zugewiesen. Gruppenalarme werden im Dashlet **Gruppenalarmstatus** *(siehe 256)* der Seite Monitor > **Dashboard-Liste** angezeigt. Sie können neue Gruppen über die Registerkarte **Gruppenalarm-Spaltennamen** in Monitor > **Monitorlisten** *(siehe 264)* erstellen. Gruppenalarmspalten werden Monitor-Sets über **Monitor-Set definieren** *(siehe 269)* zugewiesen.

Dashboardliste

Info Center > Dashboard > Dashboard-Liste

Monitor > Dashboard > Dashboard-Liste

- Mit Monitor > Alarmübersicht *(siehe 260)* und Info Center > Reporting > Berichte > Monitor-Alarmübersicht *(siehe 225)* werden ähnliche Informationen bereitgestellt.

Die Seite **Dashboard-Liste** ist die primäre Oberfläche des VSA, um Kontrolldaten, einschließlich Meldungen und Alarme, anzuzeigen. Über die Seite **Dashboard-Liste** werden konfigurierbare Kontrollfenster namens **Dashboard-Ansichten** gepflegt. Jedes Dashboard enthält einen oder mehrere Fensterbereiche mit Kontrolldaten, die als **Dashlets** bezeichnet werden. Jeder VSA-Benutzer kann seine eigenen angepassten Dashboards erstellen.

Dashboard-Ansichten und Dashlets hinzufügen

So fügen Sie ein neues Dashboard hinzu:

1. Klicken Sie auf , um eine neue **Dashboard-Ansicht** zu erstellen. Das neue Dashboard wird in einem Popup-Fenster angezeigt.
2. Geben Sie einen **Titel** und eine **Beschreibung** für das neue Dashboard ein.
3. Klicken Sie auf die Registerkarte **Dashlets hinzufügen**. In einem seitlichen Bereich wird eine Liste der Dashlets angezeigt. Mögliche Auswahlen sind:
   - **Alarmliste** *(siehe 253)*
   - **Alarm-Netzwerkstatus** *(siehe 253)*
   - **Alarm Rotator** *(siehe 255)*
   - **Alarm Ticker** *(siehe 255)*
   - **Netzwerkstatus** *(siehe 255)*
   - **Gruppenalarmstatus** *(siehe 256)*
   - **Monitor-Set-Status** *(siehe 256)*
   - **Monitorstatus** *(siehe 259)*
   - **Rechner online** *(siehe 259)*
   - **Top N – Monitoralarmliste** *(siehe 259)*

- ➢ **KES Status** *(siehe 259)*
- ➢ **KES Bedrohungen** *(siehe 260)*

4. Aktivieren Sie so viele Kontrollkästchen, wie Sie wünschen, und klicken Sie dann auf die Schaltfläche **Hinzufügen**. Der seitliche Bereich wird geschlossen, und die **Dashlets** werden in der **Dashboard-Ansicht** angezeigt.
5. Sie können die **Dashlets** innerhalb der **Dashboard-Ansicht** verschieben und ihre Größe verändern.
6. Klicken Sie auf die Registerkarte **Löschen**, um in der **Dashboard-Ansicht** angezeigte Dashlets zu löschen.
7. Klicken Sie auf , um die **Dashboard-Ansicht** zu speichern Klicken Sie auf , um die **Dashboard-Ansicht** unter einem anderen Namen und mit einer anderen Beschreibung zu speichern.
8. Klicken Sie auf **Gemeinsam nutzen**, um diese **Dashboard-Ansicht** mit anderen Benutzern und Benutzerrollen gemeinsam zu nutzen oder sie allen Benutzern für die Verwendung und Bearbeitung zur Verfügung zu stellen.

Dashlet-Optionen konfigurieren

Sie können jedes Dashlet innerhalb der **Dashboard-Ansicht** in der Größe verändern und neu positionieren. Sie können auch auf weitere Konfigurationsoptionen für jedes Dashlet zugreifen, indem Sie auf das Konfigurationssymbol in der oberen linken Ecke des Dashlet klicken. Mögliche Konfigurationsoptionen sind:

- **Titelleiste anzeigen** – Wenn diese Option aktiviert ist, wird das Dashlet mit einer Titelleiste angezeigt.
- **Titel** – Mit dieser Option geben Sie den Titel des Dashlet an.
- **Aktualisierungsfrequenz** – Gibt an, wie oft die Daten in dem Dashlet aktualisiert werden.
- **Rechner** – Filtert die Dashlets nach der Rechner-ID. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.
- **Rechnergruppe** – Filtert die Dashlets nach der Gruppen-ID. Wählen Sie `<All Groups>` aus, um alle Gruppen zu sehen, zu deren Ansicht Sie autorisiert sind.

> **Hinweis:** Dashlets sind unabhängig vom *Haupt*-**Rechner-ID-/Rechnergruppen-Filter** *(siehe 626)*, der am oberen Rand der VSA-Seite angezeigt wird.

Dashboard hinzufügen

Klicken Sie auf , um ein neues Dashboard zu erstellen Das neue Dashboard wird in einem Popup-Fenster angezeigt.

Titel

Geben Sie einen Titel für Ihr Dashboard ein und klicken Sie auf das Filtersymbol , um die Liste der im Seitenbereich angezeigten Dashboards zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Geben Sie einen anderen Titel ein, um das Dashboard umzubenennen.

Meine Dashboards

Wenn diese Option aktiviert ist, werden nur die Dashboards, deren Eigentümer Sie sind, angezeigt.

Ansicht

Zeigt die für jedes Dashboard verfügbaren Ansichtssymbole an.

– Klicken Sie auf dieses Symbol, um das Dashboard anzuzeigen.

– Klicken Sie auf dieses Symbol, um das Dashboard zu konfigurieren.

– Klicken Sie auf dieses Symbol, um das Dashboard zu löschen.

Besitzer

Der Eigentümer des Dashboards.

Titel

Der Name des Dashboards.

Beschreibung

Die Beschreibung des Dashboards.

Beim Start laden

Wenn diese Option aktiviert ist, wird das Dashboard angezeigt, wenn sich der Benutzer anmeldet. Die Auswahlen gelten nur für den gegenwärtig angemeldeten Benutzer.

Alarmliste

Dashboard > Dashboard-Liste > *Alarmliste*

Das Dashlet **Alarmliste** zeigt alle Alarme für alle Rechner-IDs an, die mit dem Rechner-ID-/Gruppen-ID-Filter des Dashlets übereinstimmen. Die neuesten Alarme werden zuerst angezeigt.

Alarm-Netzwerkstatus

Dashboard > Dashboard-Liste > *Alarm-Netzwerkstatus*

Zunächst wird im Dashlet **Alarm-Netzwerkstatus** jede Rechnergruppe als ein Symbol angezeigt. Sie können auf ein Gruppensymbol klicken, um die Rechner in dieser Gruppe anzuzeigen. Falls für einen Rechner auch nur ein einziger `Open` Alarm vorliegt, wird in dem Symbol für diesen Rechner ein rotes Ausrufezeichen angezeigt. Klicken Sie auf ein beliebiges Rechnersymbol, um ein **Alarmübersichtsfenster** *(siehe 253)* der `Open` Alarme für diesen Rechner anzuzeigen.

Alarmübersichtsfenster

Dashboard > Dashboard-Liste > *Alarm-Netzwerkstatus*

Dashboard > Dashboard-Liste > *Gruppenalarmstatus*

Dashboard > Dashboard-Liste > *Monitor-Set-Status*

Im **Alarmübersichtsfenster** wird eine gefilterte Liste der Alarmprotokoll-Datensätze angezeigt. Die Filterung richtet sich danach, wie auf das Fenster zugegriffen wurde. Ein im Alarmprotokoll aufgeführter Alarm weist nicht unbedingt auf den *aktuellen Status* eines Rechners oder Geräts hin, sondern ist vielmehr eine *Aufzeichnung* eines Alarms, der *in der Vergangenheit* aufgetreten ist. Ein Alarmprotokoll-Datensatz bleibt solange `Open`, bis Sie ihn schließen.

> **Hinweis:** Innerhalb eines Dashlet werden im **Alarmübersichtsfenster** *nur* `Open` *Alarmprotokoll-Datensätze angezeigt.* Beim Versuch, Alarme mit dem Status `Closed` innerhalb eines Dashlet zu filtern, setzt das Dashlet Ihre Auswahl auf `Open` zurück. Durch Schließen eines Alarms wird diese aus der Alarmübersichtsliste des Dashlet gelöscht. Sie können sowohl `Open` als auch `Closed` Alarme auf der **Alarmübersichtsseite** *(siehe 260)* überprüfen.

Alarme filtern

Wählen Sie in einem oder mehreren der folgenden **Alarmfilter**-Felder Werte aus bzw. geben Sie sie ein. Die Filterung tritt unmittelbar nach Auswahl oder Eingabe eines Werts in Kraft.

- **Alarm-ID** – Eine spezifische Alarm-ID
- **Monitor-Typ** – `Zähler`, `Prozess`, `Dienst`, `SNMP`, `Meldung`, `Systemprüfung`, `Sicherheit` oder `Protokoll-Monitoring`.
- **Alarmstatus** – `Open` oder `Closed`. Sie können den Status `Open` nur für einen Alarm auswählen, der in einem Dashlet **Alarmübersichtsfenster** aufgelistet wird.
- **Alarmtyp** – `Alarm` oder `Trending`.
- **Alarmtext** – Der in dem Alarm enthaltene Text Klammertext mit Sternchen, zum Beispiel: `*memory*`
- **Filteralarmzählung** – Die Anzahl der Alarme, die unter Verwendung der aktuellen Filterkriterien angezeigt werden

Alarme schließen

Es gibt zwei Möglichkeiten, Alarmprotokoll-Datensätze zu schließen:

- Klicken Sie auf den Link `Open` in der Spalte **Status** des Fensters **Alarmübersicht**.

Oder:

1. Setzen Sie die Dropdown-Liste **Alarmstatus** auf `Closed`.
2. Wählen Sie einen oder mehrere der im Seitenbereich aufgelisteten Alarme aus.
3. Klicken Sie auf die Schaltfläche **Aktualisieren**.

Alarm löschen

1. Wählen Sie einen oder mehrere der im Seitenbereich aufgelisteten Alarme aus.
2. Klicken Sie auf die Schaltfläche **Löschen...**.

Anmerkungen hinzufügen

1. Geben Sie eine Anmerkung in das Feld **Anmerkungen** ein.
2. Wählen Sie einen oder mehrere der im Seitenbereich aufgelisteten Alarme aus.
3. Klicken Sie auf die Schaltfläche **Aktualisieren**.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Alarm-ID

Listet eine vom System generierte, eindeutige ID für jeden Alarm auf. Durch Klicken auf das Erweiterungssymbol ⊞ werden spezifische Alarminformationen eingeblendet.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline

- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen. In jedem Dashlet werden alle Rechnergruppen und Rechner-IDs angezeigt, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen.

Alarmdatum

Das Datum und die Uhrzeit, zu der der Alarm erstellt wurde

Typ

Der Typ des Monitorobjekts: `Counter`, `Process`, `Service`, `SNMP`, `Alert`, `System Check`, `Security` und `Log Monitoring`.

Ticket

Falls ein Ticket für einen Alarm generiert wurde, wird ein **Ticket-ID**-Link angezeigt. Durch Klicken auf diesen Link wird das Ticket auf der Seite Ticketing > **Ticket anzeigen** *(siehe 460)* angezeigt. Falls kein Ticket für einen Alarm generiert wurde, wird der Link **Neues Ticket** angezeigt. Klicken Sie auf diesen Link, um ein Ticket für diesen Alarm zu erstellen.

Name

Der Name des Monitorobjekts

Alarm Rotator

Dashboard > Dashboard-Liste > Alarm Rotator

Im Dashlet **Alarm Rotator** werden aktuelle Alarme angezeigt, die während der letzten zehn Minuten ausgelöst wurden. Die Alarme werden kontinuierlich der Reihe nach für jeweils 10 Sekunden angezeigt. Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen.

Alarm Ticker

Dashboard > Dashboard-Liste > Alarm Ticker

Im Dashlet **Alarm Ticker** werden aktuelle Alarme angezeigt, die innerhalb einer festgelegten Zeitspanne ausgelöst wurden. Die Alarme werden der Reihe nach, ähnlich wie bei einem Ticker-Band, für jeweils 10 Sekunden angezeigt. Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen.

Netzwerkstatus

Dashboard > Dashboard-Liste > Netzwerkstatus

Das Dashlet **Netzwerkstatus** gilt spezifisch für Rechner, denen *Monitor-Sets* bzw. Geräte, denen *SNMP-Sets* zugewiesen wurden.   In diesem Dashlet werden alle Rechnergruppen und Rechner-IDs angezeigt, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen.

Über dieses Dashlet können Sie den *aktuellen Status* von Monitor-Sets auf Rechnern bzw. von SNMP-Sets auf Geräten *dynamisch* anzeigen.

Zunächst wird im Dashlet **Netzwerkstatus** jede Rechnergruppe als ein Symbol angezeigt. Sie können auf ein Gruppensymbol klicken, um die Rechner und SNMP-Geräte in dieser Gruppe anzuzeigen. Falls sich auch nur ein einziges Monitor-Set oder SNMP-Set im Alarmzustand befindet, wird in dem Symbol

für diesen Rechner bzw. dieses Gerät ein rotes Ausrufezeichen angezeigt. Klicken Sie auf ein beliebiges Rechner- oder Gerätesymbol, um eine Liste der Monitor-Set- oder SNMP-Set-Alarme anzuzeigen, die *gegenwärtig* außerhalb ihrer Alarmschwellenwerte liegen. Alarme in dieser Liste werden automatisch entfernt, sobald für das Monitor-Set bzw. das SNMP-Set wieder der Status „Kein Alarm" vorliegt.

Verworfen

Sie können einen Alarm manuell dazu zwingen, einen „Kein Alarm"-Status zurückzugeben, indem Sie für diesen Alarm auf den Link **Verwerfen** klicken. Der Alarm-Status wird wieder angezeigt, sobald das Monitor-Set bzw- SNMP-Set erneut den Alarmschwellenwert überschreitet. Wann dies geschieht, richtet sich nach den Alarmintervall-Kriterien, die für dieses Monitor-Set bzw. SNMP-Set definiert wurden.

> **Hinweis:** Das Verwerfen eines Alarm-*Status* sollte nicht mit dem Status `Open` oder `Closed` eines Alarm-*Datensatzes* im Alarmprotokoll verwechselt werden, welcher beispielsweise über das **Alarmübersichtsfenster** *(siehe 253)* angezeigt wird. Alarmprotokolleinträge können unbegrenzt `Open` bleiben, lange nachdem der Alarmstatus wieder zu „kein Alarm" zurückgekehrt ist.

Gruppenalarmstatus

Dashboard > Dashboard-Liste > Gruppenalarmstatus

Im Dashlet **Gruppenalarmstatus** werden die Alarmstatus aller **Gruppenalarm** *(siehe 619)*kategorien für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen, angezeigt. Alarme für Meldungen, Ereignisprotokoll-Meldungen, Systemprüfung und Protokoll-Monitoring werden automatisch einer **Gruppenalarm**-Kategorie zugewiesen. Beim Auslösen eines Alarms wird auch der zugehörige Gruppenalarm ausgelöst. Die Gruppenalarm-Kategorien für Monitor-Sets und SNMP-Sets werden bei der Definition der Sets manuell zugewiesen. Gruppenalarme werden im Dashlet **Gruppenalarmstatus** *(siehe 256)* der Seite Monitor > **Dashboard-Liste** angezeigt. Sie können neue Gruppen über die Registerkarte **Gruppenalarm-Spaltennamen** in Monitor > **Monitorlisten** *(siehe 264)* erstellen. Gruppenalarmspalten werden Monitor-Sets über **Monitor-Set definieren** *(siehe 269)* zugewiesen.

> **Hinweis:** Verwechseln Sie *Gruppenalarmkategorien* nicht mit *Rechnergruppen-IDs*.

- Klicken Sie auf den Link **Rechnergruppen-ID**, um den Gruppenalarmstatus aller in diese Rechnergruppen-ID eingeschlossenen Rechner-IDs und SNMP-Geräte-IDs anzuzeigen.
- Klicken Sie auf den Link **Rechner-ID/SNMP-Geräte-ID**, um ein Fenster **Monitor-Set-Status** *(siehe 256)* für die Rechner-ID und die damit verknüpften SNMP-Geräte anzuzeigen.
- Klicken Sie auf ein beliebiges rotes Symbol in der Tabelle, um das **Alarmübersichtsfenster** *(siehe 253)* für diese Kombination von *Gruppenalarmkategorie und Rechnergruppen-ID* oder *Gruppenalarmkategorie und Rechner-ID* anzuzeigen.
- Klicken Sie auf **Filtern...**, um ein Dashlet nach Gruppenalarmkategorie oder nach Rechnergruppen-ID zu filtern. Klicken Sie auf **Zurücksetzen**, um ein gefiltertes Dashlet auf seinen Standardwert zurückzusetzen. Sie können die Anzeige der Gruppenalarmkategorien auch neu anordnen.

Monitor-Set-Status

Dashboard > Dashboard-Liste > Monitor-Set-Status

- Sie können auch ein Dashlet Monitor-Set-Status über ein Dashlet Gruppenalarmstatus anzeigen, indem Sie auf einen Link Rechnergruppen-ID und anschließend auf einen Link Rechner-ID klicken.

Im Dashlet **Monitor-Set-Status** werden alle Alarme angezeigt, die dieser Rechner-ID zugewiesen sind, egal, ob sie über **Monitor-Set** *(siehe 622)*, **Alarm** *(siehe 621)*, **Systemprüfung** *(siehe 631)*, **SNMP-Set** *(siehe 276)*

oder **Protokoll-Monitoring erstellt wurden** *(siehe 626)*. Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen.

Nur Monitor-Objekte in Alarmzustand anzeigen

Wenn diese Option aktiviert ist, werden nur Monitor-Objekte mit Alarmstatus in der Liste aufgeführt.

Nur Rechner in Alarmzustand anzeigen

Wenn diese Option aktiviert ist, werden nur Rechner mit Alarmstatus in der Liste aufgeführt.

Erste Zeile mit Informationen

Auf der ersten Zeile mit Informationen wird Folgendes angezeigt:

- Das **Check-in-Status** *(see "Anmeldestatus" on seite 614)*-Symbol – Klicken Sie auf dieses Symbol, um das **Live Connect** *(siehe 393)*-Fenster anzuzeigen. Alt-klicken Sie, um die **Rechnerübersichtsseite** *(siehe 151)* anzuzeigen.
- Das Rechnerstatus-Symbol – Klicken Sie auf dieses Symbol, um das Popup-Fenster **Rechnerstatus** *(siehe 258)* anzuzeigen. In diesem Fenster können Sie eine permanente Anzeige von Diagrammen oder Tabellen der Monitor-Set-Objekte für eine bestimmte Rechner-ID festlegen. Diese Option gilt nur für Monitor-Objekte, nicht für Meldungen, Systemprüfungen oder SNMP-Sets.
- Das Erweiterungssymbol – Klicken Sie auf dieses Symbol, um alle einer Rechner-ID zugeordneten Alarme anzuzeigen.
- Das Reduzieren-Symbol – Klicken Sie auf dieses Symbol, um nur die Kopfzeilen alle einer Rechner-ID zugeordneten Alarme anzuzeigen.
- Die **Rechner-ID.Gruppen-ID** *(siehe 626)*.

Monitor-Sets

Falls einer Rechner-ID ein Monitor-Set zugewiesen ist, erscheinen unter dem Namen des Monitor-Sets folgende Angaben:

- Der ausgelöste „Alarm"- oder „Kein Alarm"-Status des Monitor-Sets
- Das Erweiterungssymbol – Klicken Sie auf dieses Symbol, um Informationen zur Erfassung und zum Schwellenwert anzuzeigen.
- Der **Schnellstatus**-Link oder das Schnelldiagramm-Symbol – Klicken Sie hierauf, um ein Popup-Fenster **Schnellstatuskontrolle** einzublenden. Mit dieser Funktion können Sie einen *beliebigen* Monitor-Set-Zähler, -Dienst oder -Prozess für eine *beliebige* Rechner-ID auswählen und sie zum gleichen Einzelanzeigefenster hinzufügen. Mithilfe von **Schnellstatus** können Sie im Handumdrehen die Leistung des gleichen Zählers, Dienstes oder Prozesses auf mehreren Rechnern vergleichen und verschiedene Monitor-Sets in einer einzelnen Ansicht anzeigen. SNMP-Sets stellen eine ähnliche **Schnellstatus**-Ansicht für ausgewählte SNMP-Objekte zur Verfügung. *Eine von Ihnen erstellte Schnellstatus-Ansicht existiert nur für die aktuelle Sitzung.* Klicken Sie auf das **Rechnerstatus** *(siehe 258)*-Symbol , um Diagrammanzeigeauswahlen permanent zu speichern.
- Das Monitor-Protokoll-Symbol – Klicken Sie auf dieses Symbol, um das **Monitor-Protokoll** *(siehe 333)* für diesen einzelnen Alarmzähler in einem Popup-Fenster anzuzeigen.
- Das Live-Monitor-Protokoll-Symbol – Klicken Sie auf dieses Symbol, um aktuelle, fortlaufende Zählerprotokollinformationen in einem Popup-Fenster anzuzeigen.
- Der Monitor-Set-Objektname
- Für ausgelöste Alarme wird der **Alarm**-Hyperlink angezeigt. Klicken Sie, um das **Alarmübersichtsfenster** *(siehe 253)* anzuzeigen. Das **Alarmübersichtsfenster** ist auf `Open` Alarme für das ausgewählte Monitor-Set-Objekt und die Rechner-ID beschränkt.

Meldungen

Wenn einer Rechner-ID ein Alarm zugewiesen wurde, werden zusammen mit jedem Alarm die

folgenden Angaben angezeigt:

- Der ausgelöste „Alarm"- oder „Kein Alarm"-Status der Benachrichtigung.
- Der Meldungstyp
- Für ausgelöste Alarme wird der **Alarm**-Hyperlink angezeigt. Klicken Sie, um das **Alarmübersichtsfenster** *(siehe 253)* anzuzeigen. Das **Alarmübersichtsfenster** ist auf `Open` Meldungen für die ausgewählte Rechner-ID beschränkt.

Systemprüfungen

Wenn einer Rechner-ID eine Systemprüfung zugewiesen wurde, werden zusammen mit jeder Systemprüfung die folgenden Angaben angezeigt:

- Der ausgelöste Alarm oder der „Kein Alarm"-Status der Systemprüfung.
- Der Typ der Systemprüfung.
- Für ausgelöste Alarme wird der **Alarm**-Hyperlink angezeigt. Klicken Sie, um das **Alarmübersichtsfenster** *(siehe 253)* anzuzeigen. Das **Alarmübersichtsfenster** ist auf `Open` Systemprüfungen für die ausgewählte Rechner-ID beschränkt.

SNMP-Geräte

Wenn einem SNMP-Gerät ein SNMP-Set zugewiesen wurde, werden zusammen mit jedem SNMP-Set-Objekt die folgenden Angaben angezeigt:

- Das Gerätestatus-Symbol – Klicken Sie auf dieses Symbol, um eine permanente Anzeige von Diagrammen oder Tabellen der Monitor-Set-Objekte für ein bestimmtes SNMP-Gerät anzuzeigen. Zeigt das **Gerätestatus** *(siehe 259)*-Popup-Fenster an
- Die IP-Adresse des SNMP-Geräts.
- Der Name des SNMP-Geräts.
- Der Name des dem SNMP-Gerät zugewiesenen SNMP-Sets. Zusammen mit jedem SNMP-Set werden die folgenden Angaben angezeigt:
  - Der ausgelöste „Alarm"- oder „Kein Alarm"-Status des SNMP-Sets.
  - Das Erweiterungssymbol ⊞ – Klicken Sie auf dieses Symbol, um Informationen zur Erfassung und zum Schwellenwert anzuzeigen.
  - Das Monitor-Protokoll-Symbol – Klicken Sie auf dieses Symbol, um das **SNMP-Protokoll** *(siehe 349)* für diesen einzelnen Alarmzähler in einem Popup-Fenster anzuzeigen.
  - Der SNMP-Set-Objektname.
  - Für ausgelöste Alarme wird der **Alarm**-Hyperlink angezeigt. Klicken Sie, um das **Alarmübersichtsfenster** *(siehe 253)* anzuzeigen. Das **Alarmübersichtsfenster** ist auf `Open` Alarme für das ausgewählte SNMP-Set-Objekt und das SNMP-Gerät beschränkt.

Rechnerstatus

Dashboard > Dashboard-Liste > Monitor-Set-Status > Rechnerstatussymbol

Im Popup-Fenster **Rechnerstatus** wählen Sie Diagramme oder Tabellen für **Monitor-Set** *(siehe 622)*-Objekte aus bzw. zeigen diese an. Das Setup ist für jede Rechner-ID spezifisch und kann permanent gespeichert werden. Dies gilt nur für Monitor-Set-Objekte. Monitor-Sets müssen einer Rechner-ID zugewiesen werden, bevor dieses Fenster geöffnet werden kann.

- Klicken Sie auf die Schaltfläche **Einrichtung...**, um Monitor-Objekte für die Anzeige auszuwählen und das Diagramm- oder Tabellenformat festzulegen.
- Klicken Sie auf **Position speichern**, um die Auswahl zu speichern und die Monitor-Objekte auf der Seite **Monitor-Set-Status** zu formatieren.

Gerätestatus

Dashboard > Dashboard-Liste > Monitor-Set-Status > Rechnerstatussymbol

Im Popup-Fenster **Gerätestatus** wählen Sie Diagramme oder Tabellen für **SNMP-Geräte** *(siehe 629)* aus bzw. zeigen diese an. Das Setup ist für jedes SNMP-Gerät spezifisch und kann permanent gespeichert werden.

- Klicken Sie auf die Schaltfläche **Einrichtung...**, um Monitor-Objekte für die Anzeige auszuwählen und das Diagramm- oder Tabellenformat festzulegen.
- Klicken Sie auf **Position speichern**, um die Auswahl zu speichern und die Monitor-Objekte auf der Seite **Monitor-Set-Status** zu formatieren.

Monitorstatus

Dashboard > Dashboard-Liste > Monitorstatus

Im Dashlet **Monitorstatus** wird ein Balkendiagramm mit der Anzahl der Alarme angezeigt, die für das ausgewählte Zeitintervall erstellt wurden. Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen. Dieses Dashlet kann über Monitor > **Dashboard-Einstellungen** *(siehe 260)* angepasst werden.

Rechner online

Dashboard > Dashboard-Liste > Rechner online

Im Diagramm **Rechner online** wird der Prozentsatz der Server und Workstations angezeigt, die gegenwärtig online sind Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen. Dieses Dashlet kann über Monitor > **Dashboard-Einstellungen** *(siehe 260)* angepasst werden.

Top N – Monitoralarmliste

Dashboard > Dashboard-Liste > Top N - Monitoralarmliste

Im Dashlet **Top N – Monitoralarmliste** wird ein Balkendiagramm angezeigt, in dem Sie ablesen können, für welche Rechner im ausgewählten Zeitintervall die *meisten* Alarme ausgelöst wurden. Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen. Das Diagramm kann bis zu zehn Rechner darstellen. Dieses Dashlet kann über Monitor > **Dashboard-Einstellungen** *(siehe 260)* angepasst werden.

KES-Status

Dashboard > Dashboard-Liste > KES-Status

Im Dashlet **KES-Status** werden verschiedene Ansichten des Sicherheitsstatus der Rechner-IDs angezeigt, die Endpoint Security-Schutz verwenden. Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen. Es sind drei Ansichten des Sicherheitsstatus möglich:

- **Rechnerkonfiguration**
- **Scandetails**
- **Profildiagramm**

Hinweis: Dieses Dashlet wird nur angezeigt, wenn das Endpoint Security-Zusatzmodul für den VSA installiert ist.

KES-Bedrohungen

Dashboard > Dashboard-Liste > KES-Bedrohungen

Im Dashlet **KES-Bedrohungen** werden verschiedene Ansichten der Sicherheitsbedrohungen für Rechner-IDs angezeigt, die Endpoint Security-Schutz verwenden. Dies gilt für alle Rechner-IDs, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen. Es sind drei Ansichten von Sicherheitsbedrohungen möglich:

- **Neueste**
- **Häufigste**
- **Profildiagramm**

> **Hinweis:** Dieses Dashlet wird nur angezeigt, wenn das Endpoint Security-Zusatzmodul für den VSA installiert ist.

Dashboard-Einstellungen

Info Center > Dashboard > Einstellungen
Monitor > Dashboard > Dashboard-Einstellungen

Über die Seite **Einstellungen** können Sie die Steuerungen für Dashlets anpassen.

- **Schalten Sie Benachrichtigungstöne für alle Popup-Monitoring-Fenster ein oder aus** – Gilt nur für das **Monitor-Set-Status** *(siehe 256)*-Dashlet.
- Der Titel und die Hintergrundfarben für **Summenliste der Monitoralarme** und **Top N-Liste der Monitoralarme** können angepasst werden. Jeder Diagrammparameter ist anpassbar. Hierzu gehören auch das Diagramm-Zeitintervall und die Anzahl der Rechner, auf die in **Top N-Liste der Monitoralarme** Bezug genommen wird.
- Über **Zonen für Rechner online anpassen** werden zwei Prozentsätze festgelegt, anhand derer Sie drei Zonen von Online-Rechnern erstellen können:
  - Der Prozentsatz der Rechner online, unterhalb dessen eine Meldungsbedingung ausgelöst wird.
  - Der zusätzliche Prozentsatz der Rechner online, unterhalb dessen eine Warnbedingung ausgelöst wird.
- **Aktualisierungszeit anzeigen**
- **Benutzerdefiniertes Dashboard-Design** – Wählen Sie den Rahmen und den Titelleistenstil für Dashlets aus.

Alarmübersicht

Monitor > Status > Alarmübersicht

- Mit Monitor > Dashboard-Liste *(siehe 251)* und Info Center > Reporting > Berichte > Monitor werden ähnliche Informationen bereitgestellt.

Auf der Seite **Alarmübersicht** werden **Alarme** *(siehe 622)* für alle Rechner-IDs angezeigt, die dem aktuellen **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* entsprechen. Sie können weitere Filter für aufgelistete Alarm unter Verwendung der Felder im Fensterbereich **Alarmfilter** einschließen. Sie können Alarme auch schließen oder erneut öffnen und ihnen Anmerkungen hinzufügen.

Alarme filtern

Wählen Sie in einem oder mehreren der folgenden **Alarmfilter**-Felder Werte aus bzw. geben Sie sie ein. Die Filterung tritt unmittelbar nach Auswahl oder Eingabe eines Werts in Kraft.

- **Alarm-ID** – Eine spezifische Alarm-ID
- **Monitor-Typ** – `Zähler`, `Prozess`, `Dienst`, `SNMP`, `Meldung`, `Systemprüfung`, `Sicherheit` oder `Protokoll-Monitoring`.
- **Alarmstatus** – `Open` oder `Closed`. Sie können den Status `Open` nur für einen Alarm auswählen, der in einem Dashlet **Alarmübersichtsfenster** aufgelistet wird.
- **Alarmtyp** – `Alarm` oder `Trending`.
- **Alarmtext** – Der in dem Alarm enthaltene Text Klammertext mit Sternchen, zum Beispiel: `*memory*`
- **Filteralarmzählung** – Die Anzahl der Alarme, die unter Verwendung der aktuellen Filterkriterien angezeigt werden

Alarme schließen

Es gibt zwei Möglichkeiten, Alarmprotokoll-Datensätze zu schließen:

- Klicken Sie auf den Link `Open` in der Spalte **Status** des Fensters **Alarmübersicht**.

Oder:

1. Setzen Sie die Dropdown-Liste **Alarmstatus** auf `Closed`.
2. Wählen Sie einen oder mehrere der im Seitenbereich aufgelisteten Alarme aus.
3. Klicken Sie auf die Schaltfläche **Aktualisieren**.

Alarm löschen

1. Wählen Sie einen oder mehrere der im Seitenbereich aufgelisteten Alarme aus.
2. Klicken Sie auf die Schaltfläche **Löschen...**.

Anmerkungen hinzufügen

1. Geben Sie eine Anmerkung in das Feld **Anmerkungen** ein.
2. Wählen Sie einen oder mehrere der im Seitenbereich aufgelisteten Alarme aus.
3. Klicken Sie auf die Schaltfläche **Aktualisieren**.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Alarm-ID

Listet eine vom System generierte, eindeutige ID für jeden Alarm auf. Durch Klicken auf das Erweiterungssymbol ⊞ werden spezifische Alarminformationen eingeblendet.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline

- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen. In jedem Dashlet werden alle Rechnergruppen und Rechner-IDs angezeigt, die dem eindeutigen Rechner-ID-/Gruppen-ID-Filter des *Dashlet* entsprechen.

Alarmdatum

Das Datum und die Uhrzeit, zu der der Alarm erstellt wurde

Typ

Der Typ des Monitorobjekts: `Counter`, `Process`, `Service`, `SNMP`, `Alert`, `System Check`, `Security` und `Log Monitoring`.

Ticket

Falls ein Ticket für einen Alarm generiert wurde, wird ein **Ticket-ID**-Link angezeigt. Durch Klicken auf diesen Link wird das Ticket auf der Seite Ticketing > **Ticket anzeigen** *(siehe 460)* angezeigt. Falls kein Ticket für einen Alarm generiert wurde, wird der Link **Neues Ticket** angezeigt. Klicken Sie auf diesen Link, um ein Ticket für diesen Alarm zu erstellen.

Name

Der Name des Monitorobjekts

Alarm unterbrechen

Monitor > Status > Alarm aussetzen

Über die Seite **Alarme aussetzen** können Sie **Alarme** *(siehe 622)* für vorgegebene Zeitspannen, einschließlich wiederkehrender Zeitperioden, aussetzen. Dadurch können Sie Aufrüstungs- und Pflegeaufgaben durchführen, ohne einen Alarm auszulösen. Wenn Alarme für eine Rechner-ID ausgesetzt sind, *sammelt der Agent weiterhin Daten, generiert jedoch keine zugehörigen Alarme*. Die Liste der auswählbaren Rechner-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem verwendeten **Scope** *(siehe 419)*.

Alle löschen

Löscht alle Zeitperioden, die für das Aussetzen von Alarmen für alle ausgewählten Rechner-IDs geplant sind.

Hinzufügen/Ersetzen

Klicken Sie auf **Hinzufügen**, um eine Zeitperiode zu planen, in der Alarme für die ausgewählten Rechner-IDs ausgesetzt werden. Klicken Sie auf **Ersetzen**, um die Zeitperioden für das Aussetzen von Alarmen, die gegenwärtig ausgewählten Rechner-IDs zugeweisen sind, zu entfernen, und sie einer neuen einzelnen Zeitperiode für das Aussetzen von Alarmen zuzuweisen.

Planung

Klicken Sie auf **Planen**, um diese Aufgabe auf ausgewählten Rechner-IDs unter Verwendung der zuvor ausgewählten Optionen zu planen.

Datum/Zeit

Geben Sie Jahr, Monat, Tag, Stunde und Minute für die Planung dieser Aufgabe ein.

Abbrechen

Löscht eine Zeitperiode, die den Datum/Uhrzeit-Parametern für das Aussetzen von Alarmen auf ausgewählten Rechner-IDs entspricht.

Periodisch ausführen

Aktivieren Sie dieses Kontrollkästchen, um diese Aufgabe zu einer wiederholten Aufgabe zu machen. Geben Sie die Anzahl der Perioden ein, die gewartet werden soll, bevor die Aufgabe erneut ausgeführt wird.

Alarme aussetzen

Wählen Sie aus, wie lange Alarme ausgesetzt werden sollen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Nächste Unterbrechung

Listet die Startzeiten auf, ab denen Alarme für Rechner-IDs ausgesetzt werden sollen.

Dauer

Listet die Dauer der Zeitperioden auf, während derer Alarme ausgesetzt werden sollen.

Wiederholen

Für periodisch wiederholte Aufgaben wird das Intervall für die Wartezeit angezeigt, bevor die Aufgabe erneut ausgeführt wird.

Live Counter

Monitor > Status > Live Counter

Auf der Seite **Live Counter** werden Live-**Leistungszählerdaten** *(siehe 620)* für die ausgewählte Rechner-ID angezeigt. Nur Rechner-IDs, denen mit **Monitor zuweisen** *(siehe 327)* ein oder mehrere Monitor-Set(s) zugewiesen wurden, werden auf dieser Seite aufgeführt. Die Liste der auswählbaren Rechner-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem verwendeten **Scope** *(siehe 419)*.

Jeder einzelne **Live Counter** wird in einem neuen Fenster angezeigt. In jedem Fenster wird ein Balkendiagramm mit 75 Datenpunkten angezeigt, die den Wert des Zählerobjekts für die angegebene **Aktualisierungsfrequenz** darstellen. Die Aktualisierungsfrequenz des Diagramms kann auf einen Wert zwischen 3 und 60 Sekunden eingestellt werden. Die neuen Daten werden ganz rechts im Diagramm angezeigt. Mit zunehmendem Alter werden die Daten weiter nach links verschoben.

Jeder Balken in dem Diagramm wird in einer eigenen Farbe angezeigt, die durch den Alarm und die Warnschwellenwerte des Monitor-Set-Zählerobjekts bestimmt werden.

- **Rot** – Bei Alarm
- **Gelb** – Wenn innerhalb des Warnschwellenwerts
- **Grün** – Wenn kein Alarm und nicht innerhalb des Warnschwellenwerts

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

(Rechner.Gruppen-ID)

Listet die **Rechner.Gruppen-IDs** *(siehe 626)* auf, die gegenwärtig dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* entsprechen und einem oder mehreren Monitor-Set(s) zugewiesen wurden. Klicken Sie auf eine Rechner-ID, um ein Monitor-Set, die Aktualisierungsfrequenz und einen oder mehrere Zähler auszuwählen.

Monitor-Set auswählen

Wählen Sie ein Monitor-Set aus.

Bildwiederholfrequenz

Geben Sie einen Wert zwischen 3 und 60 ein. Dies ist das Intervall, während dessen **Live Counter** Daten sammelt.

Zähler auswählen

Listet die in einem ausgewählten Monitor-Set enthaltenen Zähler auf. Klicken Sie auf einen Zähler-Link, um ein **Live Counter**-Fenster für diesen Zähler anzuzeigen.

Monitorlisten

Monitor > Bearbeiten > Monitorlisten

Auf der Seite **Monitorlisten** wird eine umfassende Liste aller auf dem Kaseya Server geladenen Objekte, Dienste und Prozesse gepflegt, anhand derer **Monitor-Sets** *(siehe 267)* und **SNMP-Sets** *(siehe 276)* erstellt werden. Außerdem werden auf der Seite **Monitorlisten** benutzerdefinierte **Gruppenalarme** *(siehe 619)* verwaltet.

Hinweis: Die Listen **Zählerobjekte**, **Zähler**, **Instanzen** und **Dienste** werden von **Liste nach Scan aktualisieren** *(siehe 266)* ausgefüllt. Bei den meisten Windows-Rechnern wird **Liste nach Scan aktualisieren** automatisch ausgeführt. Neben diesen Listen können auch die **Dienste** und **Prozesse** mit Daten aus dem Import eines **Monitor-Sets** *(siehe 267)* ausgefüllt werden. **MIB-OIDs** können über die Seite **SNMP-Objekt hinzufügen** *(siehe 281)* oder durch den Import eines **SNMP-Sets** *(siehe 276)* ausgefüllt werden.

Zählerobjekte

Auf dieser Registerkarte werden **Zählerobjekte** aufgelistet, die Sie in ein **Monitor-Set** *(siehe 267)* einschließen können. Monitor-Set verwendet die **PerfMon**-Kombination von **Objekt/Zähler/Instanz** *(siehe 620)*, um Zählerinformationen zu erfassen.

Hinweis: Zählerobjekte sind die primäre Referenz. Der Benutzer muss zunächst einen Datensatz des Zählerobjekts hinzufügen, bevor er Datensätze der entsprechenden Zähler oder Instanzen hinzufügt.

Zähler

Auf dieser Registerkarte werden **Zähler** aufgelistet, die Sie in ein **Monitor-Set** *(siehe 267)* einschließen können. Monitor-Set verwendet die **PerfMon**-Kombination von Objekt/Zähler/Instanz, um Zählerinformationen zu erfassen.

Zählerinstanzen

Auf dieser Registerkarte werden **Zählerinstanzen** aufgelistet, die Sie in ein **Monitor-Set** *(siehe 267)* einschließen können. Monitor-Set verwendet die **PerfMon**-Kombination von Objekt/Zähler/Instanz, um Zählerinformationen zu erfassen.

Hinweis: Windows **PerfMon** setzt voraus, dass ein Zählerobjekt mindestens einen Zähler enthält, jedoch nicht, dass auch eine Instanz verfügbar ist.

Dienste

Auf dieser Registerkarte werden Windows-**Dienste** aufgelistet, die Sie in ein **Monitor-Set** *(siehe 267)* einschließen können, um die Aktivität der Windows-Dienste zu überwachen. Diese Liste kann auch durch Ausführen von **Listen nach Scan aktualisieren** *(siehe 266)* *oder* durch den Import eines **Monitor-Sets** *(siehe 267)* ausgefüllt werden.

Prozesse

Auf dieser Registerkarte werden Windows-**Prozesse** aufgelistet, die Sie in ein **Monitor-Set** *(siehe 267)* einschließen können, um den Übergang von einem Prozess in den oder von dem aktuellen Status zu überwachen. Ein Prozess ist gleichbedeutend mit einer Anwendung. Die Prozessliste wird *nicht* durch die Funktion **Listen nach Scan aktualisieren** *(siehe 266)* ausgefüllt. Diese Liste kann durch den Import eines **Monitor-Sets** *(siehe 267)* ausgefüllt werden.

CMIB-OIDs

Auf dieser Registerkarte werden SNMP **MIB-Objekte** aufgelistet, die Sie in **SNMP-Sets** *(siehe 276)* einschließen können. SNMP-Sets überwachen die Aktivität von SNMP-Geräten. Diese Liste kann durch den Import eines **SNMP-Sets** *(siehe 276)* *oder* die Ausführung der Seite **SNMP-Objekt hinzufügen** *(siehe 281)* ausgefüllt werden. MIB-Objekte sind Referenzen zu Werten, die auf SNMP-Geräten überwacht werden können. Beispiel: Das MIB-Objekt `sysUptime` gibt zurück, wie viel Zeit seit Einschalten des Geräts verstrichen ist.

SNMP-Geräte

Auf dieser Registerkarte werden die Hauptkategorien von SNMP-Geräten definiert, die als **SNMP-Settypen** *(siehe 352)* bezeichnet werden. Dadurch können Sie SNMP-Sets bequem mehreren

SNMP-Geräten (basierend auf ihrem SNMP-Typ) zuweisen. Die Zuweisung kann entweder automatisch oder manuell erfolgen. Weitere Informationen finden Sie unter **SNMP-Dienste**.

SNMP-Dienste

Anhand dieser Registerkarte wird eine `sysServicesNumber` mit einem SNMP-Typ verknüpft. Ein SNMP-Typ wird über die Dropdown-Liste **Automatische Bereitstellung auf** in Monitor > SNMP-Sets > **SNMP-Set definieren** *(siehe 278)* mit einem SNMP-Set verknüpft. Während eines **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* werden die SNMP-Geräte automatisch für die Überwachung durch SNMP-Sets zugewiesen, falls das SNMP-Gerät eine `sysServicesNumber` zurückgibt, die mit dem von diesen SNMP-Sets verwendeten SNMP-Typ verknüpft ist. In dieser Tabelle sind vordefinierte SNMP-Typen und `sysServicesNumbers` für die wichtigsten Geräte vorgegeben. Durch Systemaktualisierungen und von Kunden selbst vorgenommene Aktualisierungen kann diese Tabelle jedoch aktualisiert werden.

Gruppenalarm-Spaltennamen

Auf dieser Registerkarte werden *benutzerdefinierte* **Gruppenalarm-Spaltennamen** gepflegt. Vordefinierte **Gruppenalarm** *(siehe 619)*-Spaltennamen werden hier nicht angezeigt. Verwenden Sie **Monitor-Sets** *(siehe 267)* und **Monitor-Sets definieren** *(siehe 269)*, um ein Monitor-Set einem beliebigen Gruppenalarm-Spaltennamen zuzuweisen. Gruppenalarme werden über die Seite **Dashboard-Liste** *(siehe 251)* angezeigt.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol, um den Text eines Listenelements zu bearbeiten.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol ✕, um ein Listenelement zu löschen.

Listen durch Scan aktualisieren

Monitor > Bearbeiten > Listen nach Scan aktualisieren

Mit der Seite **Listen nach Scan aktualisieren** werden eine oder mehrere Rechner-ID(s) gescannt und Listen von Zählerobjekten, Zählern, Instanzen und Diensten zurückgegeben, aus denen Sie beim Erstellen oder Bearbeiten eines Monitor-Sets eine Auswahl treffen können. Eine konsolidierte Liste aller gescannten Objekte wird auf der Seite Monitor > **Monitorlisten** *(siehe 264)* angezeigt. In der Regel müssen nur ein paar Rechner jedes Betriebssystemtyps gescannt werden, um eine Reihe von umfassenden Listen auf der Seite **Monitorlisten** zu erzeugen. Mit **Listen nach Scan aktualisieren** wird außerdem die Liste der Ereignistypen aktualisiert, die für das Monitoring unter Verwendung von Monitor > **Ereignisprotokoll-Meldungen** *(siehe 316)* zur Verfügung stehen. Sie können die Liste der verfügbaren Ereignistypen durch Einblenden der Seite Agent > **Ereignisprotokolleinstellungen** *(siehe 38)* anzeigen. Bei neueren Windows-Rechnern muss **Liste nach Scan aktualisieren** nicht öfter als einmal ausgeführt werden.

- **Für Windows-Rechner ab Windows 2000** – Die Ermittlung neuer Zählerobjekte wird vollständig vom Agent verwaltet. Es werden beispielsweise entfernbare Datenträger zu einem Rechner hinzugefügt. Ein neues Zählerobjekt für einen entfernbaren Datenträger wird innerhalb weniger Stunden vom Agent ermittelt. Bestimmt ein Monitor-Set das Monitoring dieses Datenträgers entweder durch Angabe des Laufwerksbuchstabens oder durch die Verwendung des Zählerobjekts `*ALL`, werden die Daten für diesen neu hinzugefügten Datenträger zurückgegeben.

Sämtliche überwachten Zähler, die angehalten werden, werden automatisch in der gleichen Ermittlungszeitspanne neu gestartet. All dies geschieht unabhängig von **Liste nach Scan aktualisieren**.

- **Bei Windows 2000 und älteren Windows-Rechnern** – Benutzer können **Liste nach Scan aktualisieren** auswählen, um neue Zählerobjekte auf diesen Rechnern zu ermitteln. Dies ist der einzige Grund, um **Liste nach Scan aktualisieren** auszuführen.

Jetzt ausführen

Führt einen sofortigen Scan aus.

Abbrechen

Klicken Sie auf **Abbrechen**, um die Ausführung dieser Aufgabe auf ausgewählten verwalteten Rechnern abzubrechen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Letzter Scan

Dieser Zeitstempel zeigt, wann der letzte Scan ausgeführt wurde. Wenn sich dieses Datum ändert, können neue Scandaten angezeigt werden.

Nächster Scan

Dieser Zeitstempel zeigt, wann der nächste Scan geplant ist. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt. Ein grünes ✓ Häkchen weist auf einen wiederholten Scan hin.

Monitor-Sets

Monitor > Bearbeiten > Monitor-Sets

Über die Seite **Monitor-Sets** können Sie Monitor-Sets hinzufügen, importieren oder ändern. Beispiel-Monitor-Sets werden bereitgestellt.

Ein Monitor-Set ist ein Satz von **Zählerobjekten**, **Zählern**, **Zählerinstanzen**, **Diensten** und **Prozessen**, anhand derer die Leistung von Rechnern überwacht werden kann. In der Regel wird jedem/jeder **Objekt/Instanz/Zähler** *(siehe 620)*, Dienst oder Prozess in einem Monitor-Set ein Schwellenwert zugewiesen. Sie können Alarme festlegen, die ausgelöst werden, wenn einer der Schwellenwerte im Monitor-Set überschritten wird. Ein Monitor-Set sollte als eine logische Gruppierung von Faktoren, die überwacht werden sollen, verstanden werden. Eine solche logische Gruppierung könnte beispielsweise die Überwachung alle zum Ausführen eines Exchange Server erforderlichen Zähler und Dienste sein. Sie können jedem Rechner, auf dem das Betriebssystem Windows 2000 oder höher ausgeführt wird, ein Monitor-Set zuweisen.

Das allgemeine Verfahren zum Arbeiten mit Monitor-Sets ist wie folgt:

1. Sie können die Objekte, Instanzen und Zähler von Monitor-Sets über **Monitorlisten** *(siehe 264)* wahlweise auch manuell aktualisieren und prüfen.
2. Erstellen und pflegen Sie Monitor-Sets über Monitor > **Monitor-Sets** *(siehe 267)*.
3. Weisen Sie Monitor-Sets über Monitor > **Monitor zuweisen** *(siehe 327)* bestimmten Rechner-IDs zu.
4. Wahlweise können Sie Standard-Monitor-Sets als *individualisierte Monitor-Sets* anpassen.
5. Die wahlweise Anpassung von Standard-Monitor-Sets erfolgt über *Auto-Lernen*.
6. Überprüfen Sie Monitor-Sets über folgende Befehle:
   - Monitor > **Monitor-Protokoll** *(siehe 333)*
   - Monitor > **Live Counter** *(siehe 263)*
   - Monitor > Dashboard > **Netzwerkstatus** *(siehe 255)*
   - Monitor > Dashboard > **Gruppenalarmstatus** *(siehe 256)*
   - Monitor > Dashboard > **Monitor-Set-Status** *(siehe 256)*
   - Info Center > Reporting > Berichte > Monitor > Monitor-Set-Bericht
   - Info Center > Reporting > Berichte > Monitor > Monitor-Aktionsprotokoll

Beispiel-Monitor-Sets

Der VSA stellt eine stetig wachsende Liste von Beispiel-Monitor-Sets zur Verfügung. Die Namen der Beispiel-Monitor-Sets beginnen mit ZC. Sie können die Beispiel-Monitor-Sets bearbeiten. Doch empfehlenswerter ist es, ein Beispiel-Monitor-Set zu kopieren und die Kopie zu bearbeiten. Die Beispiel-Monitor-Sets werden bei jeder Aktualisierung der Beispielsätze im Rahmen eines Pflegezyklus überschrieben.

Monitoring mit Apple OS X

Apple OS X unterstützt nur die Prozessüberwachung. Siehe **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Ordnerstrukturen

Monitor-Sets werden mithilfe von zwei Ordnerstrukturen im mittleren Feld unterhalb der Cabinets **Privat** und **Gemeinsam nutzen** organisiert. Verwenden Sie die folgenden Optionen, um Objekte in diesen Ordnerstrukturen zu verwalten:

Immer verfügbar

- **Ordnereigenschaften** – Zeigt den Namen, die Beschreibung und den Eigentümer eines Ordners und Ihre Zugriffsrechte zu diesem Ordner an.
- **(Filter anwenden)** – Geben Sie Text in das Bearbeitungsfeld des Filters ein und klicken Sie dann auf das Trichtersymbol, um das Filtern auf die Ordnerstrukturen anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in den Ordnerstrukturen gefunden wird.

Bei Auswahl eines Ordners

- **Ordner gemeinsam nutzen** – Der Ordner wird mit Benutzerrollen und einzelnen Benutzern freigegeben. Dies gilt nur für gemeinsam genutzte Cabinetordner.

> **Hinweis:** Richtlinien für Nutzungsrechte zu Objekten in Ordnerstrukturen finden Sie unter dem Thema **Ordnerrechte** *(siehe 125)*.

- **Ordner hinzufügen** – Erstellt einen neuen Ordner unterhalb des ausgewählten Cabinet oder Ordners.
- **Ordner löschen** – Löscht einen ausgewählten Ordner.
- **Ordner umbenennen** – Benennt einen ausgewählten Ordner um.
- **Neues Monitor-Set** – Öffnet das Fenster **Monitor-Set definieren** *(siehe 269)*, um ein neues Monitor-Set im ausgewählten Ordner der Ordnerstruktur zu erstellen.
- **Monitor-Set importieren** – Importiert ein Monitor-Set.

Bei Auswahl eines Monitor-Sets

- **Monitor-Set kopieren** – Kopiert das ausgewählte Monitor-Set.
- **Monitor-Set exportieren** – Exportiert das ausgewählte Verfahren.
- **Monitor-Set löschen** – Löscht das ausgewählte Verfahren.

Monitor-Sets erstellen

1. Wählen Sie im mittleren Fensterbereich einen Ordner aus.
2. Klicken Sie auf die Schaltfläche **Neues Monitor-Set**.
3. Geben Sie einen Namen ein.
4. Geben Sie eine Beschreibung ein.
5. Wählen Sie eine **Gruppenalarm** *(siehe 619)*-Kategorie aus der Dropdown-Liste **Gruppenalarm-Spaltenname** aus. Benutzerdefinierte Gruppenalarm-Spaltennamen werden über die Seite **Monitorlisten** *(siehe 264)* gepflegt. Gruppenalarme werden auf der Seite **Dashboard-Liste** *(siehe 251)* angezeigt.
6. Klicken Sie auf **Speichern**. Das Fenster **Monitor-Sets definieren** *(siehe 269)* wird angezeigt.

> **Hinweis:** Beispiel-Monitor-Sets werden nicht in der Dropdown-Liste **Monitor zuweisen** *(siehe 327)* > **Monitor-Set auswählen** angezeigt. Erstellen Sie eine Kopie des Beispiel-Monitor-Sets, indem Sie das Beispielset in **Monitor-Sets** *(siehe 267)* auswählen und auf die Schaltfläche **Speichern unter** klicken. Ihre Kopie des Beispiel-Monitor-Sets wird in der Dropdown-Liste angezeigt. In einem **SaaS** *(siehe 631)*-basierten VSA sind die Schaltflächen **Speichern** und **Speichern unter** verfügbar. Sie können Änderungen am Beispielsatz vornehmen und diesen sofort verwenden, da er nicht aktualisiert wird.

Monitor-Sets definieren

Monitor > Bearbeiten > Monitor-Sets

- Wählen Sie ein Monitor-Set in einem Ordner aus.

Über das Fenster **Monitor-Sets definieren** werden die in einem Monitor-Set enthaltenen Zählerobjekte, Zähler, Zählerinstanzen, Dienste und Prozesse gepflegt. Diese Sammlung wird aus einer „Masterliste“ zusammengestellt, die mit **Monitorlisten** *(siehe 264)* gepflegt wird. Beispiel-Monitor-Sets werden bereitgestellt.

Monitor-Sets

Ein Monitor-Set ist ein Satz von **Zählerobjekten**, **Zählern**, **Zählerinstanzen**, **Diensten** und **Prozessen**, anhand derer die Leistung von Rechnern überwacht werden kann. In der Regel wird jedem/jeder **Objekt/Instanz/Zähler** *(siehe 620)*, Dienst oder Prozess in einem Monitor-Set ein Schwellenwert

zugewiesen. Sie können Alarme festlegen, die ausgelöst werden, wenn einer der Schwellenwerte im Monitor-Set überschritten wird. Ein Monitor-Set sollte als eine logische Gruppierung von Faktoren, die überwacht werden sollen, verstanden werden. Eine solche logische Gruppierung könnte beispielsweise die Überwachung alle zum Ausführen eines Exchange Server erforderlichen Zähler und Dienste sein. Sie können jedem Rechner, auf dem das Betriebssystem Windows 2000 oder höher ausgeführt wird, ein Monitor-Set zuweisen.

Das allgemeine Verfahren zum Arbeiten mit Monitor-Sets ist wie folgt:

1. Sie können die Objekte, Instanzen und Zähler von Monitor-Sets über **Monitorlisten** *(siehe 264)* wahlweise auch manuell aktualisieren und prüfen.
2. Erstellen und pflegen Sie Monitor-Sets über Monitor > **Monitor-Sets** *(siehe 267)*.
3. Weisen Sie Monitor-Sets über Monitor > **Monitor zuweisen** *(siehe 327)* bestimmten Rechner-IDs zu.
4. Wahlweise können Sie Standard-Monitor-Sets als *individualisierte Monitor-Sets* anpassen.
5. Die wahlweise Anpassung von Standard-Monitor-Sets erfolgt über *Auto-Lernen*.
6. Überprüfen Sie Monitor-Sets über folgende Befehle:
   - Monitor > **Monitor-Protokoll** *(siehe 333)*
   - Monitor > **Live Counter** *(siehe 263)*
   - Monitor > Dashboard > **Netzwerkstatus** *(siehe 255)*
   - Monitor > Dashboard > **Gruppenalarmstatus** *(siehe 256)*
   - Monitor > Dashboard > **Monitor-Set-Status** *(siehe 256)*
   - Info Center > Reporting > Berichte > Monitor > Monitor-Set-Bericht
   - Info Center > Reporting > Berichte > Monitor > Monitor-Aktionsprotokoll

Klicken Sie auf die folgenden Registerkarten, um die Details für das Monitor-Set zu definieren.

- **Zähler-Schwellenwerte** *(siehe 271)*
- **Dienstprüfung** *(siehe 273)*
- **Prozessstatus** *(siehe 274)*

Name des Monitor-Sets

Geben Sie einen aussagekräftigen Namen für das Monitor-Set ein, anhand dessen Sie es in Monitor-Set-Listen identifizieren können.

Monitor-Set-Beschreibung

Beschreiben Sie das Monitor-Set genauer. Der Grund für die Erstellung des Monitor-Sets mag im Moment offensichtlich sein, doch dieser Sinn kann im Laufe der Zeit verloren gehen.

Gruppenalarm-Spaltenname

Weisen Sie dieses Monitor-Set einem **Gruppenalarm-Spaltennamen** zu. Beim Auslösen eines Monitor-Set-Alarms wird auch der zugehörige **Gruppenalarm** *(siehe 619)* ausgelöst. Gruppenalarme werden im Fensterbereich **Gruppenalarmstatus** *(siehe 256)* der Seite Monitor > **Dashboard-Liste** angezeigt.

> **Hinweis:** Die Option **Abgleichen aktivieren** *(siehe 273)* gilt für Zähler, Dienste und Prozesse.

Speichern

Speichert Änderungen an einem Datensatz.

Speichern unter

Speichert einen Datensatz unter einem neuen Namen.

Monitor-Set exportieren...

Klicken Sie auf den Link **Monitor-Set exportieren...**, um das Verfahren im XML-Format im Popup-Fenster **Monitor-Sets exportieren** anzuzeigen. Sie können es in die Zwischenablage kopieren oder in eine

Textdatei herunterladen.

Zähler-Schwellenwerte

Monitor > Bearbeiten > Monitor-Sets

- Wählen Sie ein Monitor-Set in einem Ordner aus und wählen Sie anschließend „Zähler-Schwellenwerte".

Auf der Registerkarte **Zählerschwellenwerte** definieren Sie Meldungsbedingungen für alle mit einem Monitor-Set verknüpften Leistungsobjekte/Instanzen/Zähler. Dabei handelt es sich um die gleichen Leistungsobjekte, Instanzen und Zähler, die auch beim Ausführen der Datei `PerfMon.exe` auf einem Windows-Rechner angezeigt werden.

Hinweis: Die Option **Abgleichen aktivieren** *(siehe 273)* gilt für Zähler, Dienste und Prozesse.

Leistungsobjekte, Instanzen und Zähler

Beim Einrichten von Zählerschwellenwerten in **Monitor-Sets** *(siehe 622)* ist zu beachten, wie Windows und der VSA die zu überwachenden Komponenten identifizieren:

- **Leistungsobjekt** – Eine logische Sammlung von Zählern, die mit einer Ressource oder einen Dienst verknüpft sind, der überwacht werden kann. Zum Beispiel: Prozesse, Arbeitsspeicher, physikalische Festplatten und Server haben alle ihre eigenen Sätze vordefinierter Zähler.
- **Leistungsobjekt-Instanz** – Ein Begriff, mit dem zwischen mehreren Leistungsobjekten des gleichen Typs auf einem Computer unterschieden wird. Zum Beispiel: mehrere Prozessoren oder mehrere physikalische Festplatten. Der VSA lässt Sie dieses Feld überspringen, falls nur eine Instanz eines Objekts vorliegt.
- **Leistungszähler** – Ein mit einem Leistungsobjekt und gegebenenfalls mit der Instanz verknüpftes Datenelement. Jeder ausgewählte Zähler stellt einen Wert das, der einem bestimmen Aspekt der Leistung entspricht, die für das Leistungsobjekt und die Instanz definiert wurden.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol neben einer Zeile, um diese Zeile zu bearbeiten.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol, um diesen Datensatz zu löschen.

Hinzufügen/Bearbeiten

Klicken Sie auf **Hinzufügen** oder das Bearbeitungssymbol, um einen Assistenten aufzurufen, der Sie durch die sechs Schritte zum Hinzufügen oder Bearbeiten eines Leistungszählers führt.

1. Wählen Sie ein **Objekt**, einen **Zähler** und gegebenenfalls eine **Instanz** aus den jeweiligen Dropdown-Listen aus.
   - Falls nur eine Instanz eines Leistungsobjekts vorliegt, kann das Feld **Instanz** normalerweise ignoriert werden.
   - Die zum Auswählen der Leistungsobjekte, -zähler und -instanzen verwendeten Dropdown-Listen basieren auf der „Masterliste", die auf der Seite **Monitorlisten** *(siehe 264)* gepflegt wird. Wird ein(e) Objekt/Instanz/Zähler in der entsprechenden Dropdown-Liste nicht angezeigt, können diese über **Objekt hinzufügen**, **Zähler hinzufügen** bzw. **Instanz hinzufügen** manuell hinzugefügt werden.
   - Unabhängig vom Bereich der Zählerinstanzen, die von einem Monitor-Set festgelegt wurden, zeigt die Seite **Monitor-Protokoll** *(siehe 333)* nur die Instanzen an, die auf einem

bestimmten Rechner vorhanden sind. Neu hinzugefügte Zählerinstanzen – zum Beispiel das Hinzufügen eines entfernbaren Datenträgers zu einem Rechner – werden kurze Zeit nach der Erkennung auf der Seite **Monitor-Protokoll** angezeigt, wenn sie im für die Überwachung festlegten Bereich eines Monitor-Sets enthalten sind.

- Sind mehrere Instanzen vorhanden, können Sie eine Instanz mit der Bezeichnung `_Total` hinzufügen. Mit der Instanz `_Total` geben Sie an, dass Sie den *kombinierten* Wert aller anderen Instanzen eines Leistungsobjekts *als einen einzelnen Zähler* überwachen möchten.
- Sind mehrere Instanzen vorhanden, können Sie mithilfe der Registerkarte **Monitorlisten** *(siehe 264)* > **Zählerinstanz** eine Zählerinstanz mit der Bezeichnung `*ALL` zur Liste der unterstützten Instanzen hinzufügen. Sobald sie zum gewünschten Zähler hinzugefügt wurde, wird der Wert `*ALL` in der Dropdown-Liste der diesem Zähler zugeordneten Instanzen angezeigt. Mit der Instanz `*ALL` können Sie alle Instanzen des gleichen Leistungsobjekts *unter Verwendung einzelner Zähler* überwachen.

2. Sie können wahlweise den **Namen** und die **Beschreibung** des Standard-Zählerobjekts ändern.
3. Wählen Sie die erfassten Protokolldaten aus. Falls ein numerischer Wert zurückgegeben wird, können Sie ungewünschte Protokolldaten ausblenden, indem Sie unmittelbar über oder unter dem Erfassungsschwellenwert einen Erfassungsbetreiber festlegen.
   - **Erfassungsbetreiber** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen `Changed`, `Equal` oder `NotEqual`. Für numerische Rückgabewerte lauten die Optionen `Equal`, `NotEqual`, `Over` oder `Under`.
   - **Erfassungsschwellenwert** – Legen Sie einen festen Wert fest, mit dem der Rückgabewert verglichen wird. Verwenden Sie den ausgewählten **Erfassungsbetreiber**, um festzulegen, welche Protokolldaten erfasst werden.
   - **Beispielintervall** – Bestimmt, wie häufig die Daten vom Agent an den Kaseya Server gesendet werden.
4. Geben Sie an, wann eine Meldungsbedingung eintritt.
   - **Alarm-Operator** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen `Changed`, `Equal` oder `NotEqual`. Für numerische Rückgabewerte lauten die Optionen `Equal`, `NotEqual`, `Over` oder `Under`.
   - **Alarmschwellenwert** – Legen Sie einen festen Wert fest, mit dem der Rückgabewert verglichen wird. Verwenden Sie den ausgewählten **Alarm-Operator**, um festzulegen, wann eine Meldungsbedingung eintritt.
   - **Dauer** – Geben Sie die Zeitspanne an, die die Rückgabewerte fortlaufend den Alarmschwellenwert überschreiten müssen, um die Meldungsbedingung zu generieren. Viele Meldungsbedingungen lösen nur dann einen Alarm aus, wenn das Alarmniveau über eine längere Dauer hinweg konstant bleibt.
   - **Zusätzliche Alarme übergehen für** – Unterdrücken Sie weitere Meldungsbedingungen für das gleiche Problem für die angegebene Zeitspanne. Dadurch vermeiden Sie Verwirrung, wenn für das gleiche Problem zahlreiche Meldungsbedingungen bestehen.
5. **Warnen innerhalb eines Alarmschwellenwerts von X%** – Zeigen Sie wahlweise eine Warnungs-Meldungsbedingung an, wenn der zurückgegebene Wert innerhalb eines vorgegebenen Prozentsatzes des **Alarmschwellenwerts** liegt. Das Warnsymbol ist ein gelbes Ampelsymbol .
6. Aktivieren Sie auf Wunsch einen **Trendalarm**. Trendalarme geben anhand von historischen Daten eine Prognose, wann die nächste Meldungsbedingung eintritt.
   - **Verlauf aktiviert?** – Wenn Ja, wird basierend auf den letzten 2500 aufgezeichneten Datenpunkten eine lineare Regressions-Trendlinie berechnet.
   - **Trendfenster** – Die Zeitspanne, um die die berechnete Trendlinie in die Zukunft verlängert wird. Wenn die vorausgesagte Trendlinie innerhalb der festgelegten zukünftigen Zeitspanne den Alarmschwellenwert überschreitet, wird eine Trendmeldungsbedingung generiert. In der Regel sollte ein Trendfenster auf die Zeitspanne eingestellt werden, die für die

Vorbereitung auf eine Meldungsbedingung benötigt wird. Beispiel: Ein Benutzer benötigt 10 Tage Vorwarnung, bevor eine Festplatte die Meldungsbedingung erreicht. Dies gibt ihm ausreichend Zeit für die Bestellung, Lieferung und Installation einer größeren Festplatte.

- **Zusätzliche Trendalarme übergehen für** – Unterdrückt weitere Trendmeldungsbedingungen für das gleiche Problem für die angegebene Zeitspanne.
- Trendalarme werden als ein orangefarbenes Symbol angezeigt.

Warnstatus-Meldungsbedingungen und Trendstatus-Meldungsbedingungen erzeugen keine Alarmeinträge im Alarmprotokoll, sie ändern jedoch das Aussehen des Alarmsymbols in verschiedenen Anzeigefenstern. Sie können einen Trendalarmbericht über Berichte > Monitor generieren.

Weiter

Geht zu nächsten Seite im Assistenten.

Zurück

Geht zu vorherigen Seite im Assistenten.

Speichern

Speichert Änderungen an einem Datensatz.

Abbrechen

Ignoriert die vorgenommen Änderungen und kehrt zur Liste der Datensätze zurück.

Abgleichen aktivieren

Das Kontrollkästchen **Abgleichen aktivieren** gilt wie folgt für Dienste, Zähler und Prozesse:

- **Dienste** *(siehe 271)* – Wenn diese Option aktiviert ist, werden keine Alarme erzeugt, wenn ein im Monitor-Set angegebener Dienst nicht auf einem zugewiesenen Rechner vorhanden ist. Falls diese Option nicht aktiviert ist, wird ein „Existiert nicht"-Alarm erzeugt.

> **Hinweis: Abgleichen aktivieren** *(siehe 273)* muss aktiviert sein, damit ein Dienstbereich mit dem Platzhalterzeichen * angegeben werden kann.

- **Zähler** *(siehe 271)* – Wenn diese Option aktiviert ist, werden keine Alarme erzeugt, wenn ein im Monitor-Set angegebener Zähler nicht auf einem zugewiesenen Rechner vorhanden ist. Falls diese Option nicht aktiviert ist, wird der Zähler auf der Seite **Monitor-Protokoll** *(siehe 333)* mit einem **letzten Wert** von `Not Responding` angezeigt. Es wird kein Alarm erzeugt.
- **Prozesse** *(siehe 274)* – Gilt nicht für Prozesse. Unabhängig davon, ob diese Option aktiviert bzw. nicht aktiviert ist, werden keine Alarme erzeugt, wenn ein im Monitor-Set angegebener Prozess nicht auf einem zugewiesenen Rechner vorhanden ist.

> **Hinweis:** Diese Änderung tritt nicht auf Rechnern in Kraft, denen das Monitor-Set bereits zugewiesen ist, bis das Monitor-Set neu zugewiesen wird.

Dienstprüfung

Monitor > Bearbeiten > Monitor-Sets

- Wählen Sie ein Monitor-Set in einem Ordner aus und wählen Sie anschließend „Dienstprüfung".

Auf der Registerkarte **Dienstprüfung** werden Meldungsbedingungen für einen Dienst definiert, wenn der Dienst auf einer Rechner-ID gestoppt wurde und wahlweise versucht wird, den gestoppten Dienst erneut zu starten. *Der Dienst muss auf Automatisch gesetzt werden, um von einem Monitor-Set erneut gestartet zu werden.*

Seiten auswählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol neben einer Zeile, um diese Zeile zu bearbeiten.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol, um diesen Datensatz zu löschen.

Hinzufügen/Bearbeiten

Klicken Sie auf **Hinzufügen** oder das Bearbeitungssymbol, um einen **Dienstprüfung**-Datensatz zu pflegen.

1. **Dienst** – Wählt den zu überwachenden Dienst aus der Dropdown-Liste aus.
   - Die Dropdown-Liste basiert auf der „Masterliste", die auf der Seite **Monitorlisten** *(siehe 264)* gepflegt wird. Falls ein Dienst nicht in der Dropdown-Liste aufgeführt wird, können Sie ihn manuell über **Dienst hinzufügen** hinzufügen.
   - Sie können mithilfe der Registerkarte **Monitorlisten** *(siehe 264)* > **Dienste** ein Sternchen (`*`) als Platzhalter zu den Spalten **Name** oder **Beschreibung** in der Liste der unterstützten Dienste hinzufügen. Der Platzhalterdienst wird nach dem Hinzufügen in der Dropdown-Liste der Dienste angezeigt. Durch Festlegen des Dienstes `*SQL SERVER*` werden beispielsweise alle Dienste überwacht, die die Zeichenfolge `SQL SERVER` im Dienstnamen haben.
   - Sie können mithilfe der Registerkarte **Monitorlisten** *(siehe 264)* > **Dienste** einen Dienst mit der Bezeichnung `*ALL` zu den Spalten **Name** oder **Beschreibung** in der Liste der unterstützten Dienste hinzufügen. Der Wert `*ALL` wird nach dem Hinzufügen in der Dropdown-Liste der Dienste angezeigt. Die Auswahl des Dienstes `*ALL` bedeutet, dass Sie alle Dienste überwachen möchten.

   > **Hinweis: Abgleichen aktivieren** *(siehe 273)* muss aktiviert sein, damit ein Dienstbereich mit dem Platzhalterzeichen * angegeben werden kann.

2. **Beschreibung** – Beschreibt den Dienst und den Grund für das Monitoring.
3. **Neustartversuche** – Gibt an, wie oft das System versuchen soll, den Dienst neu zu starten.
4. **Neustartintervall** – Die Zeitspanne, die zwischen Neustartversuchen gewartet werden soll. Für manche Dienste wird mehr Zeit benötigt.
5. **Zusätzliche Alarme übergehen für** – Unterdrückt weitere Meldungsbedingungen für die angegebene Zeitspanne.

Speichern

Speichert Änderungen an einem Datensatz.

Abbrechen

Ignoriert die vorgenommen Änderungen und kehrt zur Liste der Datensätze zurück.

Prozessstatus

Monitor > Bearbeiten > Monitor-Sets

- Wählen Sie ein Monitor-Set in einem Ordner aus und wählen Sie anschließend „Prozessstatus".

Auf der Registerkarte **Prozessstatus** werden Meldungsbedingungen basierend auf der Tatsache, ob ein Prozess auf einer Rechner-ID gestartet oder gestoppt wurde, definiert.

Hinweis: Die Option **Abgleichen aktivieren** *(siehe 273)* gilt für Dienste, Zähler und Prozesse.

Seiten auswählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol neben einer Zeile, um diese Zeile zu bearbeiten.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol, um diesen Datensatz zu löschen.

Hinzufügen/Bearbeiten

Klicken Sie auf **Hinzufügen** oder das Bearbeitungssymbol, um einen **Prozessstatus**-Datensatz zu pflegen.

1. **Prozess** – Wählt den zu überwachenden Prozess aus der Dropdown-Liste aus. Die Dropdown-Liste basiert auf der „Masterliste", die auf der Seite **Monitorlisten** *(siehe 264)* gepflegt wird. Falls ein Prozess nicht in der Dropdown-Liste aufgeführt wird, können Sie ihn manuell über **Prozess hinzufügen** hinzufügen.
2. **Beschreibung** – Beschreibt den Prozess und den Grund für das Monitoring.
3. **Alarm bei Übergang** – Löst eine Meldungsbedingung aus, wenn ein Prozess (Anwendung) gestartet oder gestoppt wird.
4. **Zusätzliche Alarme übergehen für** – Unterdrückt weitere Meldungsbedingungen für die angegebene Zeitspanne.

Speichern

Speichert Änderungen an einem Datensatz.

Abbrechen

Ignoriert die vorgenommen Änderungen und kehrt zur Liste der Datensätze zurück.

Monitorsymbole

Monitor > Bearbeiten > Monitor-Sets

- Wählen Sie ein Monitor-Set in einem Ordner aus und wählen Sie anschließend „Monitorsymbole".

Auf der Registerkarte **Monitorsymbole** wählen Sie Monitorsymbole aus, die bei Auftreten verschiedener Alarmstatus auf der Seite **Monitor-Protokoll** *(siehe 333)* angezeigt werden.

- **Bild für den OK-Status auswählen** – Das Standardsymbol ist ein grünes Ampelsymbol.
- **Bild für den Alarmstatus auswählen** – Das Standardsymbol ist ein rotes Ampelsymbol.
- **Bild für den Warnstatus auswählen** – Das Standardsymbol ist ein gelbes Ampelsymbol.
- **Bild für den Trendstatus auswählen** – Das Standardsymbol ist ein orangefarbenes Ampelsymbol.
- **Bild für den Nicht-Angewendet-Status auswählen** – Das Standardsymbol ist ein graues Ampelsymbol.

Speichern

Speichert Änderungen an einem Datensatz.

Zusätzliche Monitorsymbole hochladen

Wählen Sie den Link **Zusätzliche Monitorsymbole hochladen** aus, um Ihre eigenen Symbole in die Statussymbol-Dropdown-Listen hochzuladen.

Wiederherstellen

Setzt alle Monitorsymbole auf ihre Standardwerte zurück.

SNMP-Sets

Monitor > Bearbeiten > SNMP-Sets

Mit **SNMP-Sets** können Sie ein SNMP-Set hinzufügen, importieren oder ändern. Ein SNMP-Set ist ein Satz von MIB-Objekten, mit denen Sie die Leistung **SNMP-aktivierter Netzwerkgeräte** *(siehe 629)* überwachen können. Das SNMP-Protokoll wird benutzt, weil auf diesen Geräten kein Agent installiert werden kann. Sie können jedem Leistungsobjekt in einem SNMP-Set Alarmschwellenwerte zuweisen. Wenn Sie dem SNMP-Set einem Gerät zuweisen, werden Sie benachrichtigt, wenn der Alarmschwellenwert überschritten wird. Anhand der folgenden Methoden können Sie SNMP-Sets definieren und Rechner-IDs zuweisen.

- **SNMP-Schnellsets** – Erstellt ein gerätespezifisches SNMP-Set basierend auf den beim einem LAN-Watch auf diesem Gerät ermittelten Objekten und weist es zu. **SNMP-Schnellsets** *(siehe 629)* sind die einfachste Methode, SNMP-Monitoring auf einem Gerät zu implementieren.
- **SNMP-Standardsets** – Hierbei handelt es sich für gewöhnlich um generische SNMP-Sets, die auf mehrere Geräte angewendet und auf diesen gepflegt werden. Nachdem ein Schnellset erstellt wurde, kann dieses als ein Standardset gepflegt werden.
- **Individualisierte SNMP-Sets** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann manuell angepasst wurden.
- **SNMP-Auto-Lernen** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann automatisch über Auto-Lernen angepasst wurden.
- **SNMP-Typen** – Damit bezeichnet man eine Methode, SNMP-Standardsets, basierend auf dem während eines LAN-Watch festgestellten **SNMP-Typ** *(siehe 630)*, automatisch Geräten zuzuweisen.

In der Regel verwenden Sie das folgende Verfahren, um SNMP-Sets zu konfigurieren und Geräten zuzuweisen.

1. Ermitteln Sie SNMP-Geräte über Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor >**SNMP zuweisen** *(siehe 340)* den ermittelten Geräten zu. Diese können SNMP-Schnellsets, -Standardsets, individualisierte oder Auto-Lernen-Sets einschließen.
3. Zeigen Sie SNMP-Alarme mit Monitor > **SNMP-Protokoll** *(siehe 349)* oder **Dashboard-Liste** *(siehe 251)* an.

Die folgenden zusätzlichen SNMP-Funktionen stehen zur Verfügung und können in beliebiger Reihenfolge verwendet werden.

- Überprüfen Sie wahlweise die Liste aller importierten SNMP-Objekte mit Monitor > **Monitorlisten** *(siehe 264)*.
- Die Pflege von SNMP-Sets kann wahlweise mit Monitor > **SNMP-Sets** *(siehe 276)* erfolgen.
- Mit Monitor > **SNMP-Objekt hinzufügen** *(siehe 281)* können Sie wahlweise ein SNMP-Objekt hinzufügen.
- Mit Monitor > **SNMP-Typ konfigurieren** *(siehe 352)* können Sie wahlweise manuell einen SNMP-Typ einem SNMP-Gerät zuweisen.
- Mit Monitor > **SNMP-Werte einstellen** *(siehe 350)* können Sie wahlweise Werte auf SNMP-Geräte schreiben.

> **Hinweis:** Für die Implementierung des SNMP v1- und SNMP v2-Informationsabrufs von SNMP-fähigen Geräten in Anlehnung an alle geltenden Copyright-Anforderungen werden bestimmte Befehlszeilenfunktionen der Net-SNMP-Suite von Anwendungen verwendet.

Monitoring mit Apple OS X

Apple OS X unterstützt SNMP-Monitoring. Siehe **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Ordnerstrukturen

SNMP-Sets werden mithilfe von zwei Ordnerstrukturen im mittleren Feld unterhalb der Cabinets **Privat** und **Gemeinsam nutzen** organisiert. Verwenden Sie die folgenden Optionen, um Objekte in diesen Ordnerstrukturen zu verwalten:

Immer verfügbar

- **Ordnereigenschaften** – Zeigt den Namen, die Beschreibung und den Eigentümer eines Ordners und Ihre Zugriffsrechte zu diesem Ordner an.
- **(Filter anwenden)** – Geben Sie Text in das Bearbeitungsfeld des Filters ein und klicken Sie dann auf das Trichtersymbol , um das Filtern auf die Ordnerstrukturen anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in den Ordnerstrukturen gefunden wird.

Bei Auswahl eines Ordners

- **Ordner gemeinsam nutzen** – Der Ordner wird mit Benutzerrollen und einzelnen Benutzern freigegeben. Dies gilt nur für gemeinsam genutzte Cabinetordner.

> **Hinweis:** Richtlinien für Nutzungsrechte zu Objekten in Ordnerstrukturen finden Sie unter dem Thema **Ordnerrechte** *(siehe 125)*.

- **Ordner hinzufügen** – Erstellt einen neuen Ordner unterhalb des ausgewählten Cabinet oder Ordners.
- **Ordner löschen** – Löscht einen ausgewählten Ordner.
- **Ordner umbenennen** – Benennt einen ausgewählten Ordner um.
- **Neues SNMP-Set** – Öffnet das Fenster **SNMP-Set definieren** *(siehe 278)*, um ein neues Monitor-Set im ausgewählten Ordner der Ordnerstruktur zu erstellen.
- **SNMP-Set importieren** – Importiert ein Monitor-Set.

Bei Auswahl eines Monitor-Sets

- **Monitor-Set löschen** – Löscht das ausgewählte Verfahren.

SNMP-Sets erstellen

1. Wählen Sie im mittleren Fensterbereich einen Ordner aus.
2. Klicken Sie auf die Schaltfläche **Neues SNMP-Set**.
3. Geben Sie einen Namen ein.
4. Geben Sie eine Beschreibung ein.
5. Wählen Sie einen **SNMP-Typ** *(siehe 352)* aus der Dropdown-Liste **Automatische Bereitstellung auf** aus. Wenn ein LAN-Watch ein SNMP-Gerät dieses Typs vorfindet, beginnt das System automatisch mit dem Monitoring dieses SNMP-Geräts anhand dieses SNMP-Sets.
6. Wählen Sie eine **Gruppenalarm** *(siehe 619)*-Kategorie aus der Dropdown-Liste **Gruppenalarm-Spaltenname** aus. Benutzerdefinierte Gruppenalarm-Spaltennamen werden über die Seite **Monitorlisten** *(siehe 264)* gepflegt. Gruppenalarme werden auf der Seite **Dashboard-Liste** *(siehe 251)* angezeigt.
7. Klicken Sie auf **Speichern**. Das Fenster **SNMP-Set definieren** *(siehe 278)* wird angezeigt.

Hinweis: Beispiel-SNMP-Sets werden nicht in der Dropdown-Liste **SNMP zuweisen** *(siehe 340)* > **SNMP-Set auswählen** angezeigt. Erstellen Sie eine Kopie des Beispiel-SNMP-Sets, indem Sie das Beispielset in **SNMP-Sets** *(siehe 276)* auswählen und auf die Schaltfläche **Speichern unter** klicken. Ihre Kopie des Beispiel-SNMP-Sets wird in der Dropdown-Liste angezeigt. In einem **SaaS** *(siehe 631)*-basierten VSA sind die Schaltflächen **Speichern** und **Speichern unter** verfügbar. Sie können Änderungen am Beispielsatz vornehmen und diesen sofort verwenden, da er nicht aktualisiert wird.

SNMP-Set definieren

Monitor > Bearbeiten > SNMP-Sets > SNMP-Set definieren

- Wählen Sie ein SNMP-Set in einem Ordner aus.

Über die Seite **SNMP-Set definieren** werden die in einem SNMP-Set enthaltenen MIB-Objekte gepflegt.

Ein SNMP-Set ist ein Satz von MIB-Objekten, mit denen Sie die Leistung **SNMP-aktivierter Netzwerkgeräte** *(siehe 629)* überwachen können. Das SNMP-Protokoll wird benutzt, weil auf diesen Geräten kein Agent installiert werden kann. Sie können jedem Leistungsobjekt in einem SNMP-Set Alarmschwellenwerte zuweisen. Wenn Sie dem SNMP-Set einem Gerät zuweisen, werden Sie benachrichtigt, wenn der Alarmschwellenwert überschritten wird. Anhand der folgenden Methoden können Sie SNMP-Sets definieren und Rechner-IDs zuweisen.

- **SNMP-Schnellsets** – Erstellt ein gerätespezifisches SNMP-Set basierend auf den beim einem LAN-Watch auf diesem Gerät ermittelten Objekten und weist es zu. **SNMP-Schnellsets** *(siehe 629)* sind die einfachste Methode, SNMP-Monitoring auf einem Gerät zu implementieren.
- **SNMP-Standardsets** – Hierbei handelt es sich für gewöhnlich um generische SNMP-Sets, die auf mehrere Geräte angewendet und auf diesen gepflegt werden. Nachdem ein Schnellset erstellt wurde, kann dieses als ein Standardset gepflegt werden.
- **Individualisierte SNMP-Sets** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann manuell angepasst wurden.
- **SNMP-Auto-Lernen** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann automatisch über Auto-Lernen angepasst wurden.
- **SNMP-Typen** – Damit bezeichnet man eine Methode, SNMP-Standardsets, basierend auf dem während eines LAN-Watch festgestellten **SNMP-Typ** *(siehe 630)*, automatisch Geräten zuzuweisen.

In der Regel verwenden Sie das folgende Verfahren, um SNMP-Sets zu konfigurieren und Geräten zuzuweisen.

1. Ermitteln Sie SNMP-Geräte über Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor >**SNMP zuweisen** *(siehe 340)* den ermittelten Geräten zu. Diese können SNMP-Schnellsets, -Standardsets, individualisierte oder Auto-Lernen-Sets einschließen.
3. Zeigen Sie SNMP-Alarme mit Monitor > **SNMP-Protokoll** *(siehe 349)* oder **Dashboard-Liste** *(siehe 251)* an.

Die folgenden zusätzlichen SNMP-Funktionen stehen zur Verfügung und können in beliebiger Reihenfolge verwendet werden.

- Überprüfen Sie wahlweise die Liste aller importierten SNMP-Objekte mit Monitor > **Monitorlisten** *(siehe 264)*.
- Die Pflege von SNMP-Sets kann wahlweise mit Monitor > **SNMP-Sets** *(siehe 276)* erfolgen.
- Mit Monitor > **SNMP-Objekt hinzufügen** *(siehe 281)* können Sie wahlweise ein SNMP-Objekt hinzufügen.
- Mit Monitor > **SNMP-Typ konfigurieren** *(siehe 352)* können Sie wahlweise manuell einen SNMP-Typ einem SNMP-Gerät zuweisen.
- Mit Monitor > **SNMP-Werte einstellen** *(siehe 350)* können Sie wahlweise Werte auf SNMP-Geräte schreiben.

Hinweis: Für die Implementierung des SNMP v1- und SNMP v2-Informationsabrufs von SNMP-fähigen Geräten in Anlehnung an alle geltenden Copyright-Anforderungen werden bestimmte Befehlszeilenfunktionen der Net-SNMP-Suite von Anwendungen verwendet.

Klicken Sie auf die folgenden Registerkarten, um die Details für das SNMP-Set zu definieren.

- **SNMP-Sets** *(siehe 279)*
- **SNMP-Symbole** *(siehe 283)*

SNMP-Monitor-Set-Name

Geben Sie einen aussagekräftigen Namen für das SNMP-Set ein, anhand dessen Sie es in SNMP-Set-Listen identifizieren können.

SNMP-Monitor-Set-Beschreibung

Beschreiben Sie das SNMP-Set genauer. Der Grund für die Erstellung des Monitor-Sets mag im Moment offensichtlich sein, doch dieser Sinn kann im Laufe der Zeit verloren gehen.

Automatische Bereitstellung auf

Durch Auswahl eines Typs wird ein neu ermitteltes SNMP-Gerät automatisch einem **SNMP-Set-Typ** *(siehe 352)* zugewiesen, wenn eine **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*-Funktion ausgeführt wird.

Gruppenalarm-Spaltenname

Weisen Sie dieses SNMP-Set einem **Gruppenalarm-Spaltennamen** zu. Beim Auslösen eines SNMP-Set-Alarms wird auch der zugehörige Gruppenalarm ausgelöst. Gruppenalarme werden im Fensterbereich „Gruppenalarmstatus“ der Seite **Dashboard-Liste** *(siehe 251)* angezeigt.

Speichern

Speichert Änderungen an einem Datensatz.

Speichern unter

Speichert einen Datensatz unter einem neuen Namen.

SNMP-Set exportieren...

Klicken Sie auf den Link **SNMP-Set exportieren...**, um das Verfahren im XML-Format im Popup-Fenster **Monitor-Sets exportieren** anzuzeigen. Sie können es in die Zwischenablage kopieren oder in eine Textdatei herunterladen. SNMP-Sets können über die Seite **SNMP-Sets** *(siehe 276)* *importiert* werden.

SNMP-Set-Details

Monitor > Bearbeiten > SNMP-Sets > SNMP-Set definieren

- Wählen Sie ein SNMP-Set in einem Ordner aus und wählen Sie anschließend SNMP-Sets.

Über die Registerkarte **SNMP-Sets** können Sie alle mit einem SNMP-Set verknüpften MIB-Objekte pflegen.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol neben einer Zeile, um diese Zeile zu bearbeiten.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol X, um diesen Datensatz zu löschen.

Hinzufügen/Bearbeiten

Klicken Sie auf **Hinzufügen** oder das Bearbeitungssymbol, um einen Assistenten aufzurufen, der Sie durch die sechs Schritte zum Hinzufügen oder Bearbeiten des Monitoring eines MIB-Objekts führt.

1. Geben Sie die Kombination von Objekt/Version/Instanz an, die zum Abrufen von Informationen von einem SNMP-Gerät erforderlich ist.
   - **MIB-Objekt** – Wählen Sie das **MIB-Objekt** *(siehe 629)* aus. Klicken Sie auf **Objekt hinzufügen** *(siehe 281)*, um auf der Seite **Monitorlisten** *(siehe 264)* ein MIB-Objekt hinzuzufügen, das gegenwärtig nicht existiert.
   - **SNMP-Version** – Wählen Sie eine SNMP-Version aus. Version 1 wird von allen Geräten unterstützt (Standard). Version 2c definiert mehr Attribute, die zurückgegeben werden können, und verschlüsselt die Pakete an den und von dem SNMP-Agent. Wählen Sie Version 2c nur dann aus, wenn Sie sicher sind, dass das Gerät die Version 2c unterstützt.
   - **SNMP-Instanz** – Die letzte Zahl einer Objekt-ID kann auch als eine Wertetabelle statt eines einzelnen Werts ausgedrückt werden. Falls die Instanz ein einzelner Wert ist, geben Sie `0` ein. Wenn die Instanz eine Wertetabelle ist, geben Sie einen Zahlenbereich ein, wie beispielsweise `1-5,6` oder `1,3,7`.

     Hinweis: Wenn Sie nicht sicher sind, welche Zahlen für eine bestimmte SNMP-Instanz gültig sind, wählen Sie mittels Monitor > **SNMP zuweisen** *(siehe 340)* eine Rechner-ID aus, für die LAN-Watch durchgeführt wurde. Klicken Sie auf den Hyperlink „SNMP-Info" für das betreffende Gerät. Damit werden alle MIB-Objekt-IDs und die für das Gerät verfügbaren SNMP-Instanzen angezeigt.

   - **Wert zurückgegeben als** – Wenn das MIB-Objekt einen numerischen Wert zurückgibt, können Sie angeben, ob dieser Wert als eine **Summe** oder als eine **Rate pro Sekunde** zurückgegeben werden soll.
2. Sie können wahlweise den **Namen** und die **Beschreibung** des Standard-MIB-Objekts ändern.
3. Wählen Sie die erfassten Protokolldaten aus. Falls ein numerischer Wert zurückgegeben wird, können Sie ungewünschte Protokolldaten ausblenden, indem Sie unmittelbar über oder unter dem Erfassungsschwellenwert einen Erfassungsbetreiber festlegen.
   - **Erfassungsbetreiber** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen `Changed`, `Equal` oder `NotEqual`. Für numerische Rückgabewerte lauten die Optionen `Equal`, `NotEqual`, `Over` oder `Under`.
   - **Erfassungsschwellenwert** – Legen Sie einen festen Wert fest, mit dem der Rückgabewert verglichen wird. Verwenden Sie den ausgewählten **Erfassungsbetreiber**, um festzulegen, welche Protokolldaten erfasst werden.
   - **SNMP-Timeout** – Geben Sie die Anzahl der Perioden an, die der Agent auf eine Antwort vom SNMP-Gerät warten soll, bevor er aufgibt. Zwei Sekunden sind der Standardwert.
4. Geben Sie an, wann eine SNMP-Meldungsbedingung ausgelöst werden soll.
   - **Alarm-Operator** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen `Changed`, `Equal` oder `NotEqual`. Für numerische Rückgabewerte lauten die Optionen `Equal`, `NotEqual`, `Over`, `Under` oder `Percent Of`.
   - **Alarmschwellenwert** – Legt einen festen Wert fest, mit dem der Rückgabewert verglichen wird, und verwendet den ausgewählten **Alarm-Operator**, um festzulegen, wann eine Meldungsbedingung ausgelöst wird.
   - **Prozentobjekt** – Bei Auswahl der Option `Percent Of` für **Alarm-Operator** wird dieses Feld angezeigt. Geben Sie eine andere Kombination von Objekt/Version/Instanz in dieses Feld ein, deren Wert als ein hundertprozentiger Maßstab für Vergleichszwecke dienen kann.

- **Dauer** – Geben Sie die Zeitspanne an, die die Rückgabewerte fortlaufend den Alarmschwellenwert überschreiten müssen, um die Meldungsbedingung zu generieren. Viele Meldungsbedingungen lösen nur dann einen Alarm aus, wenn das Alarmniveau über eine längere Dauer hinweg konstant bleibt.
- **Zusätzliche Alarme übergehen für** – Unterdrücken Sie weitere Meldungsbedingungen für das gleiche Problem für die angegebene Zeitspanne. Dadurch vermeiden Sie Verwirrung, wenn für das gleiche Problem zahlreiche Meldungsbedingungen bestehen.

5. **Warnen innerhalb eines Alarmschwellenwerts von X%** – Zeigen Sie wahlweise eine Warnungs-Meldungsbedingung auf der Seite **Dashboard-Liste** *(siehe 251)* an, wenn der zurückgegebene Wert innerhalb eines vorgegebenen Prozentsatzes des **Alarmschwellenwerts** liegt. Das standardmäßige Warnsymbol ist ein gelbes Ampelsymbol . Siehe **SNMP-Symbole** *(siehe 283)*.
6. Aktivieren Sie auf Wunsch einen **Trendalarm**. Trendalarme geben anhand von historischen Daten eine Prognose, wann die nächste Meldungsbedingung eintritt.
   - **Verlauf aktiviert?** – Wenn Ja, wird basierend auf den letzten 2500 aufgezeichneten Datenpunkten eine lineare Regressions-Trendlinie berechnet.
   - **Trendfenster** – Die Zeitspanne, um die die berechnete Trendlinie in die Zukunft verlängert wird. Wenn die vorausgesagte Trendlinie innerhalb der festgelegten zukünftigen Zeitspanne den Alarmschwellenwert überschreitet, wird eine Trendmeldungsbedingung generiert. In der Regel sollte ein Trendfenster auf die Zeitspanne eingestellt werden, die für die Vorbereitung auf eine Meldungsbedingung benötigt wird.
   - **Zusätzliche Trendalarme übergehen für** – Unterdrückt weitere Trendmeldungsbedingungen für das gleiche Problem während der angegebenen Zeitspanne.
   - Trendalarme werden standardmäßig als ein orangefarbenes Symbol auf der Seite **Dashboard-Liste** *(siehe 251)* angezeigt. Sie können dieses Symbol auf der Registerkarte **SNMP-Symbole** *(siehe 283)* ändern.
   - Warnstatus-Alarme und Trendstatus-Alarme erzeugen keine Alarmeinträge im Alarmprotokoll, sie ändern jedoch das Aussehen des Alarmsymbols in verschiedenen Anzeigefenstern. Sie können einen Trendalarmbericht über Berichte > Monitor generieren.

Weiter

Geht zu nächsten Seite im Assistenten.

Zurück

Geht zu vorherigen Seite im Assistenten.

Speichern

Speichert Änderungen an einem Datensatz.

Abbrechen

Ignoriert die vorgenommen Änderungen und kehrt zur Liste der Datensätze zurück.

SNMP-Objekt hinzufügen

Monitor > Bearbeiten > SNMP-Objekt hinzufügen

Monitor > Bearbeiten > SNMP-Sets > SNMP-Set definieren

- Wählen Sie ein SNMP-Set in einem Ordner aus und wählen Sie anschließend SNMP-Sets > Objekt hinzufügen.

Wenn Sie Objekte zum Einschluss in ein SNMP-Set auswählen, haben Sie die Möglichkeit, ein neues SNMP-Objekt hinzuzufügen. In den meisten Fällen ist dies nicht erforderlich, da die benötigten Objekte normalerweise bei einem **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* ermittelt werden. Falls Sie jedoch ein SNMP-Objekt manuell aus einer MIB-Datei hinzufügen, so können Sie dies über Monitor > **SNMP-Objekt hinzufügen** *(siehe 281)* oder durch Klicken auf die

Schaltfläche **Objekt hinzufügen...** beim Konfigurieren eines SNMP-Sets tun.

Die Seite **SNMP MIB-Baumstruktur** lädt eine Management Information Base (MIB)-Datei und zeigt diese als eine erweiterbare *Baumstruktur* von MIB-Objekten an. Alle **MIB-Objekte** *(siehe 629)* werden gemäß ihrer Position in der MIB-Baumstruktur klassifiziert. Sobald diese Baumstruktur geladen wurde, können Sie die MIB-Objekte auswählen, die Sie auf Ihrem VSA installieren möchten. SNMP-Gerätehersteller stellen für gewöhnlich MIB-Dateien für die von ihnen hergestellten Geräte auf ihren Websites zur Verfügung.

> **Hinweis:** Sie können die komplette Liste der bereits installierten MIB-Objekte überprüfen, indem Sie die Registerkarte **MIB OIDs** in Monitor > **Monitorliste** *(siehe 264)* aufrufen. Dies ist die Liste der MIB-Objekte, die Sie gegenwärtig in ein SNMP-Set einschließen können.

Falls ein Hersteller Ihnen eine MIB-Datei zur Verfügung gestellt hat, können Sie die folgenden Schritte ausführen:

1. Laden Sie die MIB-Datei des Herstellers durch Klicken auf **MIB... laden**. Möglicherweise wird eine Meldung angezeigt, dass abhängige Dateien vorliegen, die zuerst geladen werden müssen. Diese werden wahrscheinlich ebenfalls vom Hersteller bereitgestellt.
2. Klicken Sie auf die ⊞ Erweiterungssymbole in der MIB-Baumstruktur *(siehe unten stehende Beispielabbildung)* und ermitteln Sie die gewünschten Kontrollelemente. Aktivieren Sie jedes entsprechende Kontrollkästchen.
3. Klicken Sie auf **MIB-Objekte hinzufügen**, um die ausgewählten Elemente aus Schritt 2 in die MIB-Objektliste zu verschieben.
4. Konfigurieren Sie die Einstellungen für das neue SNMP-Objekt innerhalb eines SNMP-Sets.
5. Die Anzahl der MIB-Objekte im Verzeichnis kann schnell unhandlich werden. Sobald die gewünschten MIB Objekte hinzugefügt wurden, kann die MIB-Datei entfernt werden.

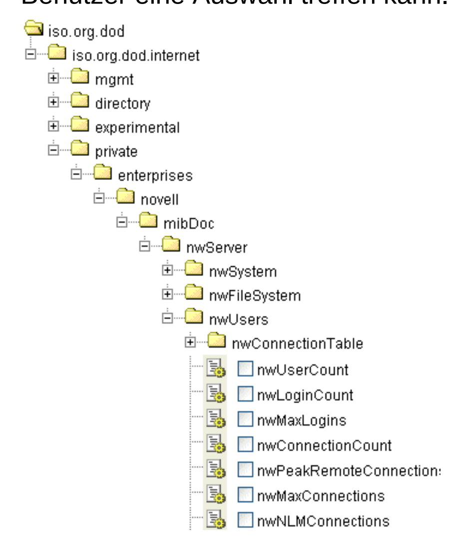
MIB laden

Klicken Sie auf **MIB laden...**, um nach einer MIB-Datei zu suchen und diese hochzuladen. Wenn beim Hinzufügen eines MIB-Objekts die folgenden standardmäßigen MIB II-Dateien nicht vorliegen, die von den meisten MIBs benötigt werden, werden diese automatisch geladen: `snmp-tc`, `snmp-smi`, `snmp-conf`, `rfc1213`, `rfc1759`. Nachdem diese Dateien geladen wurden, kann die MIB-Baumstruktur am unteren Rand der Seite **SNMP-Objekt hinzufügen** geöffnet werden. Navigieren Sie in dieser Baumstruktur, um nach den neuen Objekten zu suchen, die der Benutzer auswählen kann. Die meisten MIBs privater Hersteller werden im Ordner `Private` installiert. *Siehe nachstehende Beispielabbildung*.

> **Hinweis:**Die MIB-Datei kann jederzeit geladen und entfernt werden. Dies hat *keinen* Einfluss auf MIB-Objekte, die in SNMP-Sets verwendet werden.

MIB-Baumstruktur

Die MIB-Baumstruktur repräsentiert alle gegenwärtig geladenen MIB-Dateiobjekte, aus denen der Benutzer eine Auswahl treffen kann.



MIB Objekte hinzufügen

Klicken Sie auf **MIB-Objekte hinzufügen**, um ausgewählte Objekte zur VSA-Liste von MIB-Objekten hinzuzufügen, die mit **SNMP-Set definieren** *(siehe 278)* überwacht werden können.

MIB entfernen

Nachdem Sie die gewünschten Auswahlen getroffen haben, kann die MIB-Datei entfernt werden. Der MIB-Baum kann mit der Zeit so an Umfang zunehmen, dass er schwer zu navigieren ist. Klicken Sie auf **MIB entfernen**, um den Baum zu bereinigen.

SNMP-Symbole

Monitor > SNMP-Sets

- **Wählen Sie ein SNMP-Set in einem Ordner aus und wählen Sie anschließend SNMP-Symbole.**

Auf der Registerkarte **SNMP-Symbole** wählen Sie SNMP-Symbole aus, die bei Auftreten verschiedener Alarmstatus auf der Seite **Dashboard-Liste** *(siehe 251)* angezeigt werden.

- **Bild für den OK-Status auswählen** – Das Standardsymbol ist ein grünes Ampelsymbol .
- **Bild für den Alarmstatus auswählen** – Das Standardsymbol ist ein rotes Ampelsymbol .
- **Bild für den Warnstatus auswählen** – Das Standardsymbol ist ein gelbes Ampelsymbol .
- **Bild für den Trendstatus auswählen** – Das Standardsymbol ist ein orangefarbenes Ampelsymbol .
- **Bild für den Nicht-Angewendet-Status auswählen** – Das Standardsymbol ist ein graues Ampelsymbol .

Speichern

Speichert Änderungen an einem Datensatz.

Zusätzliche Monitorsymbole hochladen

Wählen Sie den Link **Zusätzliche Monitorsymbole hochladen** aus, um Ihre eigenen Symbole in die Statussymbol-Dropdown-Listen hochzuladen.

Wiederherstellen

Setzt alle SNMP-Symbole auf ihre Standardwerte zurück.

Meldungen

Monitor > Agent-Monitoring > Meldungen

Über die Seite **Meldungen** können Sie im Handumdrehen Meldungen für typische **Meldungsbedingungen** *(siehe 621)* definieren, die in einer IT-Umgebung vorgefunden werden. So ist beispielsweise geringer Plattenspeicherplatz ein häufiges Problem bei verwalteten Rechnern. Bei Auswahl des Meldungstyps `Low Disk` wird ein einzelnes zusätzliches Feld angezeigt, in dem Sie den `% free space`-Schwellenwert definieren können. Anschließend können Sie diese Meldung unmittelbar auf jede auf der Seite **Meldungen** angezeigte Rechner-ID anwenden und die Reaktion auf die Meldung festlegen.

> **Hinweis: Monitor-Sets** *(siehe 622)* stellen eine komplexere Methode für das Monitoring von Meldungsbedingungen dar. Typische Meldungsbedingungen sollten über die Seite **Meldungen** definiert werden.

Meldungsfunktion auswählen

Wählen Sie einen Meldungstyp aus der Dropdown-Liste **Meldungsfunktion auswählen** aus.

- **Übersicht** *(siehe 284)*
- **Agentstatus** *(siehe 286)*
- **Anwendungsänderungen** *(siehe 289)*
- **Dateien abrufen** *(siehe 292)*
- **Hardware-Änderungen** *(siehe 295)*
- **Plattenkapazität niedrig** *(siehe 297)*
- **Fehlschlagen des Skriptings** *(siehe 299)*
- **Schutzverletzung** *(siehe 302)*
- **Neuer Agent installiert** *(siehe 304)*
- **Patch-Meldung** *(siehe 306)*
- **Backup-Meldung** *(siehe 310)*
- **System** *(siehe 314)*

Meldungen – Übersicht

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Summary` aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Auf der Seite **Meldungen – Übersicht** (siehe 284) wird angezeigt, welche Meldungen für welchen Rechner aktiviert sind. Sie können Einstellungen anwenden oder löschen bzw. aktivierte Meldungseinstellungen kopieren. Hier können Sie im Einzelnen:

- Einstellungen für Alarme, Tickets und E-Mail-Hinweise *für alle aktivierten Meldungstypen gleichzeitig* auf ausgewählten Rechnern anwenden oder löschen
- Alle aktivierten Meldungseinstellungen von einer ausgewählten Rechner-ID oder Rechner-ID-Vorlage **kopieren** und sie auf mehrere Rechner-IDs anwenden

> **Hinweis:** Sie können nur Meldungen ändern oder löschen, die ursprünglich mit der Option **Kopieren** oder aber *über andere Meldungsseiten* aktiviert wurden.

Obgleich Sie über diese Seite keine Agent-Verfahren zuweisen können, werden im Seitenbereich Agent-Verfahrenszuweisungen angezeigt.

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen

Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Kopie

Nur aktiv, wenn **Übersicht** ausgewählt ist. Mit **Kopieren** werden alle Einstellungen dieses Meldungstyps für eine einzelne Rechner-ID, die durch Klicken auf **Meldungseinstellungen kopieren von <Rechner_ID> auf alle ausgewählten Rechner-IDs** ausgewählt wurden, kopiert und auf alle anderen markierten Rechner-IDs angewendet.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Meldungstyp

Listet alle Meldungstypen auf, die Sie über die Seite Monitor > **Meldungen** *(siehe 284)* einer Rechner-ID zuweisen können. Zeigt beliebige Agent-Verfahrenszuweisungen für diese Rechner-ID an.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden Das Wort `disabled` wird angezeigt, wenn dieser Rechner-ID keine Meldungen dieses Meldungstyps zugewiesen sind.

Meldungen – Agent-Status

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- **Wählen Sie `Agent Status` aus der Dropdown-Liste** Meldungsfunktion auswählen **aus.**

Die Seite **Meldungen – Agent-Status** (siehe 286) löst eine Meldung aus, wenn ein Agent offline ist, erstmals online geht, oder wenn jemand die Fernsteuerung des ausgewählten Rechners deaktiviert hat.

Online-/Offline-Meldungen für Agents

Online-/Offline-Meldungen werden nicht durch das Hochfahren und Herunterfahren des Rechners ausgelöst. Sie treten nur auf, wenn der Rechner hochgefahren wird und sich der Agentprozess nicht anmelden kann. Der Agentprozess wurde zum Beispiel möglicherweise beendet oder der Agent kann keine Verbindung zum Netzwerk herstellen.

> **Hinweis:** Wann immer der Kaseya Server-Dienst stoppt, setzt das System alle Online-/Offline-Meldungen für Agents aus. Wenn der Kaseya Server für mehr als 30 Sekunden stoppt, werden die Online-/Offline-Meldungen für Agents für eine Stunde nach dem Neustart des Kaseya Server ausgesetzt. Anstatt fortwährend zu versuchen, eine Verbindung zum Kaseya Server herzustellen, wenn der Kaseya Server ausgeschaltet ist, werden die Agents nach den ersten paar Versuchen, eine Verbindung herzustellen, in einen Ruhemodus versetzt. Durch das Aussetzen der Meldungen für eine Stunde werden irreführende Offline-Meldungen für Agents vermieden, wenn der Kaseya Server wieder hochgefahren wird.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitor-Meldungs-E-Mails können gesendet und formatiert werden:

- **1 – Meldung, wenn ein einzelner Agent offline geht**
- **2 – Meldung, wenn Benutzer Fernsteuerung deaktivieren**
- **3 – Meldung, wenn Agent online geht** – Der Online-Alarm für Agents tritt nur auf, wenn für den gleichen Rechner auch eine Offline-Meldung für Agents festgelegt wurde.

- **4 – Meldung, wenn mehrere Agents in derselben Gruppe offline gehen** – Wenn mehr als eine Offline-Meldung zur gleichen Zeit ausgelöst wird, wird die E-Mail-Benachrichtigung nach Gruppe konsolidiert.

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `Agent Status`-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind. Ein ● in einer nummerierten Spalte gibt an, dass eine Variable mit dem Meldungstyp, der dieser Nummer entspricht, verwendet werden kann.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung	1	2	3	4
<um>	#at#	Alarmzeit	●	●	●	●
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.	●	●	●	●
<gr>	#gr#	Gruppen-ID	●	●	●	●
<id>	#id#	Rechner-ID	●	●	●	
<mc>	#mc#	Anzahl der Rechner, die offline gehen				●
<ml>	#ml#	Liste der Rechner, die offline gehen				●
<qt>	#qt#	Offlinezeit/Onlinezeit/Zeit remote deaktiviert	●	●	●	●
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●	●
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●	●

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Der Agent hat sich seit <N> <Perioden> nicht eingecheckt

Wenn diese Option aktiviert ist, wird eine Meldung ausgelöst, wenn sich ein Agent für den angegebenen Zeitraum nicht eingecheckt hat.

Benachrichtigen, wenn Agent online geht

Wenn diese Option aktiviert ist, wird eine Meldung ausgelöst, wenn ein Agent online geht.

Benachrichtigen, wenn Benutzer Remote Control deaktiviert

Wenn diese Option aktiviert ist, wird eine Meldung ausgelöst, wenn der Benutzer die Fernsteuerung deaktiviert.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Offlinezeit

Zeigt den Zeitraum an, den eine Rechner-ID offline sein muss, bevor eine Meldungsbedingung eintritt.

Wiederherstellungszeit

Angabe, wie lange weitere Meldungsbedingungen unterdrückt werden sollen, nachdem die erste gemeldet wurde. Dadurch wird verhindert, dass mehrere Alarme für das gleiche Problem erzeugt werden.

Agent geht online

Zeigt ein Häkchen ✔ an, wenn eine Meldung gesendet wird, wenn ein Agent online geht.

Fernsteuerung deaktiviert

Zeigt ein Häkchen ✔ an, wenn eine Meldung gesendet wird, wenn der Benutzer die Fernsteuerung deaktiviert.

Meldungen – Anwendungsänderungen

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Application Changes` aus der Dropdown-Liste Meldungsfunktion auswählen aus.
- Mit Inventarisierung > Hinzufügen/Entfernen *(siehe 157)* und Berichte > Software werden ähnliche Informationen bereitgestellt.

Die Seite **Meldungen – Anwendungsänderungen** (siehe 289) löst eine Meldung aus, wenn auf ausgewählten Rechnern eine Anwendung installiert oder entfernt wird. Sie können die Verzeichnisse angeben, die vom Auslösen einer Meldung ausgeschlossen werden sollen. Diese Meldung basiert auf der **letzten Inventarisierung** *(siehe 615)*.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitoring-Meldungs-E-Mails können gesendet und formatiert werden:

- **Meldung, wenn sich die Anwendungsliste ändert**

Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle Application Changes-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	**Innerhalb eines Verfahrens**	**Beschreibung**
<um>	#at#	Alarmzeit
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<il>	#il#	Liste der neu installierten Anwendungen
<rl>	#rl#	Liste der neu entfernten Anwendungen
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Verfahren ausführen nach Warnung

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Benachrichtigen, wenn Audit neue Anwendung als installiert erkennt

Wenn diese Option aktiviert ist, liegt eine Meldungsbedingung vor, wenn eine neue Anwendung installiert wird.

Benachrichtigen, wenn Audit vorhandene Anwendung als gelöscht erkennt

Wenn diese Option aktiviert ist, liegt eine Meldungsbedingung vor, wenn eine vorhandene Anwendung gelöscht wird.

Verzeichnisse ausschließen

Sie können die Verzeichnisse angeben, die vom Auslösen einer Meldung ausgeschlossen werden sollen. Der Ausschließen-Pfad kann das Sternchen (*) als Stellvertreterzeichen enthalten. Beim Ausschließen eines Ordners werden auch alle darin enthaltenen Unterordner ausgeschlossen. Wenn Sie beispielsweise `*\windows\*` ausschließen, werden c:\Windows und alle Unterordner dieses Ordners ausgeschlossen. Sie können die aktuelle Liste der Anwendungen um weitere Anwendungen ergänzen, die Liste ersetzen oder sie entfernen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut

anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Installierte Anwendungen

Zeigt ein Häkchen ✓ an, wenn eine Meldung gesendet wird, wenn eine Anwendung installiert wird.

Entfernte Anwendungen

Zeigt ein Häkchen ✓ an, wenn eine Meldung gesendet wird, wenn eine Anwendung entfernt wird.

(Ausschließen)

Listet die Verzeichnisse auf, die vom Senden eines Alarms ausgeschlossen werden, wenn eine Anwendung installiert oder entfernt wird.

Meldungen – Dateien abrufen

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Get Files` aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Die Seite **Meldungen – Dateien abrufen** (siehe 292) löst eine Meldung aus, wenn der Befehl **getFile()** oder **getFileInDirectoryPath()** eines Verfahrens ausgeführt und nach dem Hochladen der Datei festgestellt wird, dass diese sich von der auf dem Kaseya Server gespeicherten Kopie unterscheidet. Liegt auf dem Kaseya Server keine vorherige Kopie vor, wird der Alarm erstellt. Sobald eine **Datei abrufen**-Meldung für eine Rechner-ID definiert wurde, ist diese Meldung *für alle Agent-Verfahren aktiv*, die einen **Datei abrufen**-Befehl verwenden, und wird auf dieser Rechner-ID ausgeführt.

> **Hinweis:** Der VSA gibt die Meldung nur dann aus, wenn die Option **Meldung senden, wenn die Datei geändert wurde** in dem Verfahren aktiviert wurde. Deaktivieren Sie Meldungen für bestimmte Dateien im Agent-Verfahrenseditor, indem Sie eine der Optionen für „ohne Meldung" auswählen.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitoring-Meldungs-E-Mails können gesendet und formatiert werden:

- Meldung, wenn eine Datei, die mit **Datei abrufen** abgerufen wurde, seit dem letzten Abruf geändert wurde
- Meldung, wenn eine Datei, die mit **Datei abrufen** abgerufen wurde, seit dem letzten Abruf nicht geändert wurde

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `Get Files`-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<um>	#at#	Alarmzeit
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<fn>	#fn#	Dateiname
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<sn>	#sn#	Name des Verfahrens, durch das die Datei aufgerufen wurde
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Verfahren ausführen nach Warnung

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.

- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Meldungen – Hardwareänderungen

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie Hardware Changes aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Die Seite **Meldungen – Hardwareänderungen** (siehe 295) löst eine Meldung aus, wenn sich die Hardwarekonfiguration auf den ausgewählten Rechnern ändert. Die ermittelten Hardwareänderungen umfassen das Hinzufügen oder Entfernen von RAM, PCI-Geräten und Plattenlaufwerken. Dieser Alarm basiert auf der **letzten Inventarisierung** *(siehe 615)*.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitoring-Meldungs-E-Mails können gesendet und formatiert werden:

- **1 – Meldung, wenn ein Laufwerk oder eine PCI-Karte hinzugefügt oder entfernt wird**
- **2 – Meldung, wenn sich die Größe des installierten RAM ändert**

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle Hardware Changes-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind. Ein ● in einer nummerierten Spalte gibt an, dass eine Variable mit dem Meldungstyp, der dieser Nummer entspricht, verwendet werden kann.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung	1	2
<um>	#at#	Alarmzeit	●	●
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.	●	●
<gr>	#gr#	Gruppen-ID	●	●
<ha>	#ha#	Liste der hinzugefügten Hardware	●	
<Stunde>	#hr#	Liste der entfernten Hardware	●	
<id>	#id#	Rechner-ID	●	●
<rn>	#rn#	Neue RAM-Größe		●
<ro>	#ro#	Alte RAM-Größe		●
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Meldungen – Geringer Speicher

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Low Disk` aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Die Seite **Meldungen – Geringer Plattenspeicher** (siehe 297) löst eine Meldung aus, wenn der verfügbare Plattenspeicher unter einen vorgegebenen Prozentsatz des freien Plattenspeicherplatzes fällt. Es wird kein weiterer Geringer Speicher-Alarm erstellt, es sei denn, der geringe Speicherplatz des Zielgeräts wird korrigiert oder der Alarm wird gelöscht und dann erneut angewendet. Diese Meldung basiert auf der **letzten Inventarisierung** *(siehe 615)*.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitor-Meldungs-E-Mails können gesendet und formatiert werden:

- **Benachrichtigen, wenn der freie Plattenspeicherplatz unter einen gegebenen Prozentsatz fällt**

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `Low Disk`-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<um>	#at#	Alarmzeit
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie

		<db-vMachine.ComputerName>.
<df>	#df#	Freier Plattenspeicherplatz
<dl>	#dl#	Laufwerksbuchstabe
<dt>	#dt#	Gesamter Plattenspeicherplatz
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<pf>	#pf#	Prozentsatz des freien Speicherplatzes
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.

- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Meldung senden, wenn auf den ausgewählten Rechnern weniger als <N> % freier Speicherplatz auf einer beliebigen Festplattenpartition übrig ist

Ein Alarm wird ausgelöst, wenn der freie Speicherplatz des Rechners unter den angegebenen Prozentsatz füllt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits
Agent online
Agent online und Benutzer gegenwärtig angemeldet.
Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
Agent ist gegenwärtig offline
Agent hat nie eingecheckt.
Agent ist online, aber die Fernsteuerung wurde deaktiviert.
Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Meldungen – Fehlschlagen des Agent-Verfahrens

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Agent Procedure Failure` aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Die Seite **Meldungen – Fehlgeschlagene Agent-Verfahren** (siehe 299) löst eine Meldung aus, wenn die Ausführung eines Agent-Verfahrens auf einem verwalteten Rechner fehlschlägt. Wenn Sie beispielsweise einen Dateinamen, Verzeichnispfad oder Registrierungsschlüssel in einem Agent-Verfahren angeben und das Verfahren dann auf einer Rechner-ID ausführen, für die diese Werte ungültig sind, können Sie unter Verwendung dieser Seite darüber benachrichtigt werden.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Alarm-E-Mails können gesendet und formatiert werden:

- **E-Mail-Nachricht formatieren, die durch Meldungen wegen Fehlschlagen des Agent-Verfahrens erzeugt wurde**

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `Agent Procedure Failure`-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<um>	#at#	Alarmzeit
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<em>	#em#	Verfahrens-Fehlermeldung
<en>	#en#	Name des Verfahrens, durch das die Datei aufgerufen wurde
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System >

Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Meldungen – Schutzverletzung

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Protection Violation` aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Die Seite **Meldungen – Schutzverletzung** (siehe 302) löst eine Meldung aus, wenn eine Datei geändert wird oder eine Schutzverletzung auf einem verwalteten Rechner festgestellt wird. Mögliche Optionen sind **Verteilte Datei wurde auf Agent geändert und aktualisiert**, **Dateizugriffsverletzung festgestellt** und **Netzwerkzugriffsverletzung festgestellt**.

Voraussetzungen

- Agent-Verfahren > **Datei verteilen** *(siehe 135)*
- Inventarisierung > **Dateizugriff** *(siehe 83)*
- Inventarisierung > **Netzwerkzugriff** *(siehe 84)*

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Alarm-E-Mails können gesendet und formatiert werden:

- **E-Mail-Nachricht formatieren, die durch Schutzverletzungs-Meldungen erzeugt wurde**

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `Protection Violation`-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<um>	#at#	Alarmzeit
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<pv>	#pv#	Beschreibung der Verletzung aus Agent-Protokoll
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail

		gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Verteilte Datei wurde auf Agent geändert und aktualisiert

Wenn diese Option aktiviert ist, wird eine Meldung ausgelöst, wenn eine Datei mit Verfahren > **Verteilte Datei** *(siehe 135)* auf dem verwalteten Rechner geändert wird. Der Agent verifiziert die verteilte Datei bei jedem **vollen Check-in** *(siehe 616)*.

Dateizugriffsverletzung festgestellt

Wenn diese Option aktiviert ist, wird eine Meldung ausgelöst, wenn ein Zugriffsversuch für eine Datei unternommen wird, die mit Inventarisierung > **Dateizugriff** *(siehe 83)* blockiert wurde.

Netzwerkzugriffsverletzung festgestellt

Wenn diese Option aktiviert ist, wird eine Meldung ausgelöst, wenn ein Versuch unternommen wird, über eine mit Inventarisierung > **Netzwerkzugriff** *(siehe 84)* als blockiert festgelegte Anwendung auf eine interne oder externe Internetsite zuzugreifen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Meldungen – Neuer Agent installiert

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- **Wählen Sie** `New Agent Installed` **aus der Dropdown-Liste** Meldungsfunktion auswählen **aus.**

Die Seite **Neuer Agent installiert** (siehe 304) löst eine Meldungen aus, wenn auf einem verwalteten

Rechner ein neuer Agent durch ausgewählte *Rechnergruppen* installiert wird.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitor-Meldungs-E-Mails können gesendet und formatiert werden:

- **Agent hat das erste Mal eingecheckt**

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `New Agent Installed`-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<um>	#at#	Alarmzeit
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<ct>	#ct#	Uhrzeit, zu der Agent das erste Mal eingecheckt hat
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen

Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Rechnergruppe

Listet Rechnergruppen auf. Alle Rechner-IDs sind mit einer Gruppen-ID und optional einer Untergruppen-ID verknüpft.

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Meldungen – Patch-Meldung

Patch-Management > Konfigurieren >Patch-Meldung

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Patch Alert` aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Die Seite **Meldungen – Patch-Meldung** (siehe 306) löst eine Meldung für Patch-Managementereignisse auf verwalteten Rechnern aus.

- Ein neues Patch ist für die ausgewählte Rechner-ID verfügbar.
- Eine Patch-Installation ist auf der ausgewählten Rechner-ID fehlgeschlagen.
- Die Anmeldeinformationen des Agents sind ungültig oder fehlen für die ausgewählte Rechner-ID.
- Automatische Windows-Aktualisierung wurde geändert.

So erstellen Sie eine Patch-Meldung:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen

➢ **E**-Mail-Empfänger

2. Legen Sie weitere E-Mail-Parameter fest.
3. Legen Sie weitere Patch-meldungsspezifische Parameter fest.
4. Markieren Sie die Rechner-IDs, auf die der Alarm angewendet werden soll.
5. Klicken Sie auf die Schaltfläche **Apply**.

So brechen Sie eine Patch-Meldung ab:

1. Aktivieren Sie das Kontrollkästchen für die Rechner-ID.
2. Klicken Sie auf die Schaltfläche **Löschen**.

   Die neben der Rechner-ID aufgeführten Meldungsinformationen werden gelöscht.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Patch-Meldungs-E-Mails können gesendet und formatiert werden:

- **1 – Neues Patch verfügbar**
- **2 – Patch-Installation fehlgeschlagen**
- **3 – Patch-Bestätigungsrichtlinien aktualisiert**
- **4 – Ungültige Agent-Anmeldeinformationen**
- **5 – Konfiguration des automatischen Windows Updates geändert**

> **Hinweis:** Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle **Patch-Meldungs**-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind. Ein ● in einer nummerierten Spalte gibt an, dass eine Variable mit dem Meldungstyp, der dieser Nummer entspricht, verwendet werden kann.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung	1	2	3	4	5
<um>	#at#	Alarmzeit	●	●	●	●	●
<au>	#au#	Änderung der automatischen Aktualisierung					●
<bl>	#bl#	Neue Berichtsliste			●		
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.	●	●	●	●	●
<fi>	#fi#	Fehlgeschlagene Berichts-ID		●			
<gr>	#gr#	Gruppen-ID	●	●		●	●
<ic>	#ic#	Ungültiger Anmeldetyp				●	
<id>	#id#	Rechner-ID	●	●		●	●
<pl>	#pl#	Neue Patch-Liste	●				
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●	●	●

	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●	●	●

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Patch-Meldungsparameter

Das System kann eine Meldung für die folgenden Meldungsbedingungen für eine ausgewählte Rechner-ID auslösen:

- **Neues Patch ist verfügbar**
- **Patch-Installation schlägt fehl**
- **Agent-Anmeldedaten sind ungültig oder fehlen**

> **Hinweis:** Agent-**Anmeldedaten** *(siehe 614)* sind für die Installation von Patches nicht erforderlich, **es sei denn**, die Dateiquelle des Rechners wurde mit `Pulled from file server using UNC path` konfiguriert. Falls Agent-Anmeldedaten zugewiesen sind, werden diese als Anmeldedaten für einen lokalen Rechner validiert, ohne auf die **Dateiquellen**-Konfiguration Bezug zu nehmen. Wenn diese Validierung fehlschlägt, wird eine Meldung ausgelöst. Falls die **Dateiquelle** des Rechners mit `Pulled from file server using UNC path` konfiguriert wurde, sind die Anmeldedaten erforderlich. Wenn sie fehlen, wird ein Alarm ausgelöst. Falls die Anmeldedaten vorliegen, werden sie als Anmeldedaten für einen lokalen Rechner und als Anmeldedaten für ein Netzwerk validiert. Wenn eine dieser Validierungen fehlschlägt, wird ein Alarm ausgelöst.

- **Automatisches Windows Update geändert**

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol neben einer Rechner-ID, um automatisch Kopfzeilenparameter einzustellen, die mit denjenigen der ausgewählten Rechner-ID übereinstimmen.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Bestätigungsrichtlinie aktualisiert

Zeigt die erste Zeile mit Daten an. Dies ist eine Systemmeldung, die mit keinen einzelnen Rechnern verknüpft ist. Es wird eine Meldung generiert, wenn ein neuer Patch zu allen Patch-Regeln hinzugefügt wird. Ein NN-- in der **ATSE**-Spalte gibt an, dass Sie keine Meldung und kein Ticket für diese Zeile festlegen können. Sie können einen E-Mail-Empfänger angeben. Sie können ein Agent-Verfahren auf einem angegebenen Rechner ausführen. Siehe Bestätigung gemäß Richtlinie.

ATSE

Der den Rechner-IDs zugewiesene ATSE-Antwortcode:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Verfahren ausführen

- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Neues Patch

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wenn ein neues Patch für diese Rechner-ID verfügbar ist.

Installation fehlgeschlagen

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wenn eine Patch-Installation für diese Rechner-ID fehlgeschlagen ist.

Ungültige Anmeldeinformationen

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wenn die Anmeldeinformationen für diese Rechner-ID ungültig sind.

Win AU geändert

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wenn die Gruppenregel für **Automatische Windows-Aktualisierung** auf dem verwalteten Rechner von der in Patch-Management > Automatische Windows-Aktualisierung festgelegten Einstellung geändert wird.

> **Hinweis:** Unabhängig von dieser Meldungseinstellung wird ein Protokolleintrag im Protokoll der Konfigurationsänderungen vorgenommen.

Meldungen – Sicherungsmeldung

Sicherung > Sicherungsmeldung

Monitor > Agent-Monitoring > Meldungen *(siehe 284)*

- Wählen Sie `Backup Alert` aus der Dropdown-Liste Meldungsfunktion auswählen aus.

Die Seite **Meldungen – Sicherungsmeldung** (siehe 310) löst eine Meldung für Sicherungsereignisse auf verwalteten Rechnern aus.

Die Liste der auswählbaren Rechner-IDs basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem verwendeten **Scope** *(siehe 419)*. Damit diese Seite angezeigt wird, muss über die Seite Sicherung > Installieren/Entfernen Sicherungssoftware auf den Rechner-IDs installiert worden sein.

So erstellen Sie einen Sicherungsalarm:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
2. Legen Sie weitere E-Mail-Parameter fest.
3. Legen Sie weitere sicherungsalarmspezifische Parameter fest.
4. Markieren Sie die Rechner-IDs, auf die der Alarm angewendet werden soll.
5. Klicken Sie auf die Schaltfläche **Apply**.

So brechen Sie eine Patch-Meldung ab:

1. Aktivieren Sie das Kontrollkästchen für die Rechner-ID.
2. Klicken Sie auf die Schaltfläche **Löschen**.

Die neben der Rechner-ID aufgeführten Meldungsinformationen werden gelöscht.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Sicherungsalarm-E-Mails können gesendet und formatiert werden:

- **Backup fehlgeschlagen**
- **Wiederkehrendes Backup übersprungen, wenn Rechner offline**
- **Backup erfolgreich abgeschlossen**
- **Vollständiges Backup erfolgreich abgeschlossen**
- **Freier Platz für Abbildspeicherort unten**
- **Überprüfen Sie, ob das Backup fehlgeschlagen ist**

> **Hinweis:** Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `Backup Alert`-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<um>	#at#	Alarmzeit
<be>	#be#	Sicherung fehlgeschlagen-Fehlermeldung
<bt>	#bt#	Sicherungstyp
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<im>	#im#	Speicherort des Sicherungsabbilds
<mf>	#mf#	freier Speicherplatz in Megabyte
<sk>	#sk#	Anzahl der übersprungenen Sicherungen
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Sicherungsalarm-Parameter

Das System löst einen Alarm aus, wann immer es auf eine von vier Sicherungsmeldungsbedingungen für eine bestimmte Rechner-ID stößt:

- **Beliebige Sicherung abgeschlossen** – Meldung, wenn eine beliebige Datenträger- oder Ordnersicherung erfolgreich abgeschlossen wurde.
- **Vollständige Sicherung abgeschlossen** – Meldung, wenn eine vollständige Datenträger- oder Ordnersicherung erfolgreich abgeschlossen wurde.
- **Sicherung fehlgeschlagen** – Meldung, wenn eine Datenträger- oder Ordnersicherung aus irgendeinem Grund vor dem Abschluss abbrach. In der Regel bricht eine Sicherung ab, wenn ein Rechner mittendrin ausgeschaltet wird oder die Netzwerkverbindung zum Dateiserver, auf den durch den Abbildspeicherort verwiesen wird, verloren geht.
- **Periodische Sicherung übersprungen, wenn Rechner<N> Mal offline** – Meldung, wenn die Option **Überspringen, wenn Rechner offline ist** unter Datenträgersicherung planen aktiviert ist und die Sicherung die angegebene Anzahl von Malen neu geplant wurde, weil der Rechner offline ist. Verwenden Sie diesen Alarm, damit Sie darauf hingewiesen werden, wenn die Sicherungen nicht einmal starten, weil der Rechner zu der für die Datenträgersicherung geplanten Zeit ausgeschaltet war.

- **Freier Platz für Abbildspeicherort unter <N> MB** – Meldung, wenn auf der zum Speichern von Sicherungen verwendeten Festplatte weniger als die angegebene Anzahl von Megabyte freier Speicherplatz ist.

Drei weitere Parameter können festgelegt werden:

- **Hinzufügen** – Fügt Meldungsparameter zu ausgewählten Rechner-IDs hinzu, wenn **Anwenden** gewählt wird, ohne dass bereits vorhandene Parameter gelöscht werden.
- **Ersetzen** – Ersetzt Meldungsparameter auf ausgewählten Rechner-IDs bei Auswahl von **Anwenden**.
- **Entfernen** – Löscht Meldungsparameter von ausgewählten Rechner-IDs. Klicken Sie *zuerst* auf das Bearbeitungssymbol neben einer Rechner-ID-Gruppe, um die zu löschenden Meldungsparameter auszuwählen.

Hinweis: Sie können für jeden Sicherungsmeldungstyp andere Meldungs-E-Mail-Adressen angeben. Auf diese Weise können Sie an einen Benutzer „Sicherung abgeschlossen"-Meldungen und an einen anderen Benutzer „Sicherung fehlgeschlagen"-Meldungen senden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Hinweis: Andere Symbolbilder werden angezeigt, wenn dieses Zusatzmodul auf einem 5.x VSA installiert wurde. Auf der Seite Fernsteuerung > **Kontrollrechner** wird eine Legende der spezifischen Symbole angezeigt, die von Ihrem VSA-System verwendet werden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Beliebige abgeschlossen

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wann immer eine Sicherung für diese Rechner-ID abgeschlossen ist.

Vollständig abgeschlossen

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wenn eine vollständige Sicherung für diese Rechner-ID abgeschlossen ist.

Sicherung fehlgeschlagen

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wann immer eine Sicherung für diese Rechner-ID fehlschlägt.

Sicherung übersprungen

Wenn diese Option aktiviert ist, wird ein Alarm ausgelöst, wann immer eine Sicherung für diese Rechner-ID übersprungen wird.

Meldungen – System

Monitor > Agent-Monitoring > **Meldungen** *(siehe 284)*

- Wählen Sie `System` aus der Dropdown-Liste **Meldungsfunktion auswählen** aus.

Die Seite **Meldungen – System** (siehe 314) löst eine Meldungen für ausgewählte Ereignisse auf dem *Kaseya Server* aus. Durch Auswahl der Seite **Meldungen – System** wird keine Liste der verwalteten Rechner angezeigt. Die aufgelisteten Ereignisse beziehen sich nur auf den Kaseya Server. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitor-Meldungs-E-Mails können gesendet und formatiert werden:

- **1 – Adminkonto manuell von einem Hauptadmin deaktiviert**
- **2 – Adminkonto wurde wegen Überschreiten des Schwellenwerts der fehlgeschlagenen Anmeldungen deaktiviert**
- **3 – KServer gestoppt**
- **4 – Datenbank-Backup fehlgeschlagen**
- **5 – E-Mail-Leseprogramm fehlgeschlagen (nur Ticketing-Modul)**

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle `System`-Meldungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind. Ein ● in einer nummerierten Spalte gibt an, dass eine Variable mit dem Meldungstyp, der dieser Nummer entspricht, verwendet werden kann.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung	1	2	3	4	5
<an>	#an#	deaktivierter VSA-Benutzername	●	●			
<um>	#at#	Alarmzeit	●	●	●	●	●
<bf>	#bf#	Datenbanksicherungsfehlerdaten				●	

<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.	●	●	●	●	●
<el>	#el#	E.Mail-Leseprogramm-Fehlermeldung					●
<fc>	#fc#	Wert, der den Zähler für fehlgeschlagene Anmeldeversuche ausgelöst hat	●	●			
<fe>	#fe#	Zeit, zu der das Konto neu aktiviert wurde	●	●			
<kn>	#kn#	Kaseya Server-IP/Name	●	●	●		
<ms>	#ms#	Typ des deaktivierten VSA-Benutzers (Haupt oder Standard)	●	●			
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●			
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●			

Anwenden

Klicken Sie auf **Anwenden**, um die Meldungsparameter auf das System anzuwenden.

Löschen

Klicken Sie auf **Löschen**, um alle Meldungsparameter vom System zu löschen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Adminkonto deaktiviert

Wenn diese Option aktiviert ist, wird eine Meldung ausgelöst, wenn ein VSA-Benutzerkonto manuell

oder automatisch deaktiviert wird.

KServer wurde gestoppt

Wenn diese Option aktiviert ist, wird eine E-Mail-Benachrichtigung ausgelöst, wenn der Kaseya Server stoppt.

Backup der Systemdatenbank fehlgeschlagen

Wenn diese Option aktiviert ist, wird eine E-Mail-Benachrichtigung ausgelöst, wenn die Sicherung der Kaseya Server-Datenbank fehlschlägt.

E-Mail-Programm in Ticketing fehlgeschlagen

Wenn diese Option aktiviert ist, wird eine E-Mail-Benachrichtigung ausgelöst, wenn das Ticketing > **E-Mail-Leseprogramm** *(siehe 472)* fehlschlägt.

System-Meldungen gesendet an

Zeigt die E-Mail-Empfänger an, an die Systemmeldungen gesendet werden.

Ereignisprotokoll-Meldungen

Monitor > Agent-Monitoring > Ereignisprotokoll-Meldungen

Die Seite **Meldungen – Ereignisprotokolle** löst eine Meldung aus, wenn ein Ereignisprotokolleintrag für einen ausgewählten Rechner vorgegebenen Kriterien entspricht. Nach Auswahl des **Ereignisprotokolltyps** können Sie die durch den **Ereignissatz** und die **Ereigniskategorie** vorgegebenen Meldungsbedingungen filtern. Sie legen dann die Meldungsaktion fest, die als Reaktion auf die angegebene Meldungsbedingung ergriffen wird.

> **Hinweis:** Sie können Ereignisprotokolle direkt anzeigen. Klicken Sie auf einem Windows-Rechner auf **Start**, **Systemsteuerung**, **Verwaltung** und dann auf **Ereignisanzeige**. Klicken Sie auf **Anwendung**, **Sicherheit** oder **System**, um die Ereignisse in jedem Protokoll anzuzeigen.

Ereignis-Sätze

Da die Anzahl der Ereignisse in Windows-**Ereignisprotokollen** *(siehe 618)* riesig ist, verwendet der VSA einen Datensatztyp namens **Ereignissatz**, um nach Meldungsbedingungen zu filtern. Ereignissätze enthalten eine oder mehrere **Bedingungen**. Jede Bedingung enthält Filter für verschiedene Felder in einem **Ereignisprotokolleintrag**. Die Feld sind **Quelle**, **Kategorie**, **Ereignis-ID**, **Benutzer** und **Beschreibung**. Ein **Ereignisprotokoll** *(siehe 618)*eintrag muss alle Feldfilter einer Bedingung erfüllen, um als Übereinstimmung zu gelten. Ein Feld mit einem Sternchen (*) bedeutet, dass jede Zeichenfolge, selbst eine leere Zeichenfolge, als Übereinstimmung gilt. Eine Übereinstimmung auch nur *einer* der Bedingungen in einem Ereignissatz ist ausreichend, um eine Meldung für einen Rechner auszulösen, auf den dieser Ereignissatz angewendet wurde. Weitere Hinweise zum Konfigurieren von Ereignissätzen finden Sie unter Monitor > Ereignisprotokoll-Meldungen > **Ereignissätze bearbeiten** *(siehe 320)*.

Beispiel-Ereignissätze

Es wird eine stetig wachsende Liste von Beispiel-Ereignissätzen zur Verfügung gestellt. Die Namen der Beispiel-Ereignissätze beginnen mit ZC. Sie können die Beispiel-Ereignissätze bearbeiten. Doch empfehlenswerter ist es, einen Beispiel-Ereignissatz zu kopieren und die Kopie zu bearbeiten. Die Beispiel-Ereignissätze werden bei jeder Aktualisierung der Beispielsätze im Rahmen eines Pflegezyklus überschrieben.

Globale Ereignisprotokollliste

Jeder Agent verarbeitet zwar alle Ereignisse, die auf einer "Blacklist" aufgeführten Ereignisse werden

jedoch *nicht* auf den VSA-Server hochgeladen. Es gibt zwei "Blacklists". Eine wird periodisch von Kaseya aktualisiert und trägt die Bezeichnung `EvLogBlkList.xml.`. Die zweite mit dem Namen `EvLogBlkListEx.xml` kann vom Dienstanbieter verwaltet werden und wird nicht von Kaseya aktualisiert. Beide befinden sich im Verzeichnis `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles`. Die Alarmermittlung und -verarbeitung werden fortgesetzt, ungeachtet dessen, ob sich die Einträge in der Erfassungs-Blacklist befinden oder nicht.

Fluterkennung

Wenn 1000 Ereignisse (ohne Zählung der **Blacklist-Ereignisse** *(siehe 619)*) von einem Agent *innerhalb einer Stunde* auf den Kaseya Server hochgeladen werden, wird die weitere Erfassung von Ereignissen dieses Protokolltyps für den Rest der Stunde angehalten. Ein neues Ereignis wird in das Ereignisprotokoll eingefügt, um die Aussetzung der Erfassung zu verzeichnen. An Ende der Stunde wird die Erfassung automatisch wieder aufgenommen. Dies verhindert, dass der Kaseya Server von kurzfristigen Schwerlasten überschwemmt wird. Die Alarmermittlung und -verarbeitung wird ungeachtet einer ausgesetzten Erfassung fortgesetzt.

Monitor-Assistent-Symbol für Ereignisätze

Ein Monitor-Assistent--Symbol wird neben dem Ereignisprotokolleintrag im VSA und in **Live Connect** angezeigt. Wenn Sie den Cursor über das Monitorassistent-Symbol eines Protokolleintrags bewegen, wird ein Assistent angezeigt. Der Assistent ermöglicht Ihnen auf Basis dieses Protokolleintrags ein neues Kriterium für den Ereignissatz zu erstellen. Das neue Ereignissatz-Kriterium kann zu jedem neuen oder bestehenden Ereignissatz hinzugefügt werden. Der neue oder geänderte Ereignissatz wird sofort auf den Rechner angewendet, der die Quelle dieses Protokolleintrags war. Wird ein bestehender Ereignissatz geändert, so sind alle Rechner davon betroffen, denen dieser Ereignissatz zugeordnet ist. Das Monitor-Assistent-Symbol wird angezeigt in:

- Agent > **Agent-Protokolle** *(siehe 35)*
- Live Connect > Ereignisanzeige
- Live Connect > Agent-Daten > Ereignisprotokoll

Siehe Monitor > **Ereignisprotokoll-Meldungen** *(siehe 316)* – hier ist jedes im Assistenten angezeigte Feld beschrieben.

Konfigurieren und Zuweisen von Ereignisprotokoll-Meldungen

1. Sie können optional die Ereignisprotokollierung für Rechner, die Sie überwachen möchten, über Agent > **Ereignisprotokolleinstellungen** *(siehe 38)* aktivieren. Rot markierte **Ereigniskategorien** (EWISFCV) geben an, dass diese Ereigniskategorien nicht vom VSA gesammelt werden. **Ereignisprotokoll-Meldungen werden auch generiert, wenn die Ereignisprotokolle nicht von VSA gesammelt werden.**
2. Wählen Sie den **Ereignissatz**, den **Ereignisprotokoll-Typ** und andere Parameter über die Kopfzeilenregisterkarte Ereignisprotokoll-Meldungen > **Ereignissatz zuweisen** *(siehe 319)* aus.
3. Klicken Sie optional auf die Schaltfläche **Bearbeiten** auf der Kopfzeilenregisterkarte **Ereignissatz zuweisen**, um **die Meldungsbedingungen für die zugewiesenen Ereignissätze zu erstellen oder ändern** *(siehe 320)*.
4. Legen Sie über die Kopfzeilenregisterkarte Ereignisprotokoll-Meldungen > **Meldungsaktionen einrichten** *(siehe 320)* die Aktionen fest, die als Reaktion auf eine Meldungsbedingung ergriffen werden.
5. Klicken Sie alternativ auf die Schaltfläche **E-Mail formatieren** auf der Kopfzeilenregisterkarte **Meldungsaktionen einrichten**, um **das Format von E-Mail-Meldungen für Ereignissätze zu ändern** *(siehe 320)*.
6. Wählen Sie die Rechner aus, auf die ein Ereignissatz angewendet werden soll.
7. Klicken Sie auf die Schaltfläche **Apply**.

Aktionen

- **Anwenden** – Wendet einen ausgewählten Ereignissatz auf ausgewählte Rechner-IDs an. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.
- **Löschen** – Entfernt den ausgewählten Ereignissatz von den ausgewählten Rechner-IDs.
- **Alle löschen** – Entfernt alle Ereignissatzeinstellungen von ausgewählten Rechner-IDs.

Seitenbereich

Im Seitenbereich werden die gleichen Spalten angezeigt wie in der ausgewählten Kopfzeilenregisterkarte.

- **Alle auswählen/Alle abwählen** – Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.
- **Check-in-Status** – Diese Symbole geben den Agent-Check-in-Status jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **Rechner.Gruppen-ID** – Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.
- **Bearbeitungssymbol** – Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.
- **Protokolltyp** – Der Typ des überwachten Ereignisprotokolls.
- **ATSE** – Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:
  - A = **A**larm erstellen
  - T = **T**icket erstellen
  - S = Agent-Verfahren ausführen
  - E = **E**-Mail-Empfänger
- **EWISFCV** – Die überwachte Ereigniskategorie.
- **E-Mail-Adresse** – Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden.
- **Ereignissatz** – Der dieser Rechner-ID zugewiesene Ereignissatz. Sie können mehrere Ereignissätze der gleichen Rechner-ID zuweisen.
- **Intervall** – Angabe, wie oft ein Ereignis innerhalb der festgelegten Zeitspannen eintritt. Gilt nur, wenn die Option **Warnen, wenn dieses Ereignis N> Mal innerhalb von <N> <Perioden> eintritt** aktiviert ist. Es wird `Missing` angezeigt, wenn die Option **Warnen, wenn dieses Ereignis nicht innerhalb von<N> <Perioden> eintritt** aktiviert wurde. Es wird `1` angezeigt, wenn die Option**Warnen, wenn dieses Ereignis ein einziges Mal eintritt** aktiviert wurde.
- **Dauer** – Angabe, wie oft ein Ereignis eintreten muss, um eine Meldungsbedingung auszulösen. Gilt nur, wenn die Option **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden> eintritt** oder **Warnen, wenn dieses Ereignis nicht innerhalb von <N> <Perioden> eintritt** aktiviert wurden.

- **Wiederherstellen** – Zeigt an, wie lange gewartet werden muss, bevor neue Meldungsbedingungen für die gleiche Kombination von Ereignissatz und Ereigniskategorie ausgelöst werden. Gilt nur, wenn mit **Zusätzliche Alarme übergehen für <N> <Perioden>** eine Wiederherstellungsperiode größer als Null angegeben wurde.

Registerkarte „Ereignissatz zuweisen"

Monitor > Agent-Monitoring > Ereignisprotokoll-Meldungen > Registerkarte „Ereignissatz zuweisen"

Verwenden Sie die Kopfzeilenregisterkarte **Ereignissatz zuweisen**, um den Ereignissatz, den Ereignisprotokolltyp und andere Parameter für einen Ereignissatz auszuwählen. Sie können auch Rechner auswählen und Ereignissätze zuweisen, wenn diese Kopfzeilenregisterkarte ausgewählt ist.

Ereignisprotokollalarm erstellen

1. Wählen Sie auf der Seite Monitor > **Ereignisprotokoll-Meldungen** die Registerkarte **Ereignissatz zuweisen** aus.
2. Wählen Sie ein Element aus der Dropdown-Liste **Ereignisprotokolltyp auswählen** aus.
3. Wählen Sie den **Ereignissatz** *(siehe 320)*-Filter aus, der zum Filtern der Ereignisse verwendet wird, die Meldungen auslösen. Standardmäßig ist <All Events> ausgewählt.

> **Hinweis:** Sie können einen neuen Ereignissatz erstellen oder einen vorhandenen Ereignissatz durch Klicken auf die Schaltfläche **Bearbeiten** bearbeiten.

4. Aktivieren Sie das Kontrollkästchen neben einer der folgenden **Ereigniskategorien**:
   - Fehler
   - WARNUNG
   - Informationen
   - Erfolgs-Audit
   - Fehler-Audit
   - Kritisch – betrifft nur Vista, Windows 7 und Windows Server 2008
   - Ausführlich – betrifft nur Vista, Windows 7 und Windows Server 2008

> **Hinweis:** Rote Zeichen zeigen eine deaktivierte Protokollierung an. Die Sammlung der Ereignisprotokolle kann vom VSA für einen bestimmten Rechner deaktiviert worden sein. Dies richtet sich nach den mit Agent > **Ereignisprotokolleinstellungen** *(siehe 38)* definierten Einstellungen. Für bestimmte Rechner sind möglicherweise nicht alle Ereigniskategorien (EWISFCV) verfügbar, wie beispielsweise die Ereigniskategorien Kritisch und Verbose. **Ereignisprotokoll-Meldungen werden auch generiert, wenn die Ereignisprotokolle nicht von VSA gesammelt werden.**

5. Geben Sie die *Häufigkeit* der Meldungsbedingung an, die zum Auslösen einer Meldung erforderlich ist:
   - **Warnen, wenn dieses Ereignis ein einziges Mal eintritt**
   - **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden>** eintritt.
   - **Warnen, wenn dieses Ereignis nicht innerhalb von <N> <Perioden>** eintritt.
   - **Zusätzliche Alarme nicht beachten für <N> <Perioden>**.
6. Klicken Sie auf die Optionsfelder **Hinzufügen** oder **Ersetzen**.
   - Durch **Hinzufügen** wird der ausgewählte Ereignissatz zur Liste der Ereignissätze hinzugefügt, die bereits ausgewählten Rechnern zugeordnet sind.
   - Durch **Ersetzen** wird die gesamte Liste an zugewiesenen Ereignissätzen auf ausgewählten Rechnern mit dem ausgewählten Ereignissatz ersetzt.

7. Wählen Sie die Registerkarte **Meldungsaktionen einrichten**, um die Aktionen auszuwählen, die als Reaktion auf die angegebenen Meldungsbedingungen ergriffen werden.
8. Klicken Sie auf **Anwenden**, um die ausgewählten Ereignistypmeldungen ausgewählten Rechner-IDs zuzuweisen.

> **Hinweis:** Klicken Sie auf **Entfernen**, um alle Ereignissatzmeldungen von ausgewählten Rechner-IDs zu entfernen. Sie müssen nicht auf die Schaltfläche **Anwenden** klicken.

Registerkarte „Meldungsaktionen einrichten"

Monitor > Agent-Monitoring > Ereignisprotokoll-Meldungen > Registerkarte „Meldungsaktionen einrichten"

Verwenden Sie die Registerkarte **Meldungsaktionen einrichten**, um die Aktionen festzulegen, die als Reaktion auf eine Ereignissatz-Meldungsbedingung ergriffen werden. Sie können auch Rechner auswählen und Ereignissätze zuweisen, wenn diese Kopfzeilenregisterkarte ausgewählt ist.

- **Alarm erstellen** – Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.
- **Ticket erstellen** – Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.
- **Skript ausführen** – Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.
- **E-Mail-Empfänger** – Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.
  - Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
  - Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für Benutzer mit Master-Rolle angezeigt.
  - Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
  - Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
  - Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
  - E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Ereignissätze bearbeiten

Monitor > Agent-Monitoring > Ereignisprotokoll-Meldungen *(siehe 316)*

- Wählen Sie `<New Event Set>` aus der Dropdown-Liste Ereignisse für Übereinstimmungen oder Übergehung definieren. Das Popup-Fenster Ereignissatz bearbeiten wird eingeblendet.

Ereignissätze bearbeiten filtert das Auslösen von Meldungen basierend auf dem Monitoring von Ereignissen in Ereignisprotokollen, die durch das Windows-Betriebssystem eines verwalteten Rechners gepflegt werden. Sie können einer Rechner-ID mehrere Ereignissätze zuweisen.

Ereignissätze enthalten eine oder mehrere **Bedingungen**. Jede Bedingung enthält Filter für verschiedene Felder in einem **Ereignisprotokolleintrag**. Die Feld sind **Quelle**, **Kategorie**, **Ereignis-ID**, **Benutzer** und **Beschreibung**. Ein **Ereignisprotokoll** *(siehe 618)*eintrag muss alle Feldfilter einer Bedingung erfüllen, um als Übereinstimmung zu gelten. Ein Feld mit einem Sternchen (*) bedeutet, dass jede Zeichenfolge, selbst eine leere Zeichenfolge, als Übereinstimmung gilt. Eine Übereinstimmung auch nur *einer* der Bedingungen in einem Ereignissatz ist ausreichend, um eine Meldung für einen Rechner auszulösen, auf den dieser Ereignissatz angewendet wurde.

> **Hinweis:** Werden einem Ereignissatz zwei Bedingungen hinzugefügt, so werden diese normalerweise als eine OR-Anweisung interpretiert. Wird für eine eine Übereinstimmung erzielt, wird ein Alarm ausgelöst. Die Ausnahme ist, wenn die Option **Warnen, wenn dieses Ereignis nicht innerhalb von<N> <Perioden> eintritt** aktiviert wurde. In diesem Falls sollten die zwei Bedingungen als eine AND-Anweisung interpretiert werden. Beide Bedingungen dürfen *nicht* innerhalb der angegebenen Zeitspanne auftreten, um eine Meldung auszulösen.
>
> **Hinweis:** Sie können Ereignisprotokolle direkt anzeigen. Klicken Sie auf einem Windows-Rechner auf **Start**, **Systemsteuerung**, **Verwaltung** und dann auf **Ereignisanzeige**. Klicken Sie auf **Anwendung**, **Sicherheit** oder **System**, um die Ereignisse in diesem Protokoll anzuzeigen. Doppelklicken Sie auf ein Ereignis, um dessen **Eigenschaften**-Fenster anzuzeigen. Sie können Text im **Eigenschaften**-Fenster jedes Ereignisses kopieren und in die **Ereignissatz bearbeiten**-Felder einfügen.

So erstellen Sie einen neuen Ereignissatz:

1. Wählen Sie die Seite Monitor > **Ereignisprotokoll-Meldungen** aus.
2. Wählen Sie einen **Ereignisprotokolltyp** aus der zweiten Dropdown-Liste.
3. Wählen Sie `<New Event Set>` aus der Dropdown-Liste **Ereignisse für Übereinstimmungen oder Übergehung definieren.** Das Popup-Fenster **Ereignissatz bearbeiten** wird eingeblendet. Zum Erstellen eines neuen Ereignissatzes haben Sie die folgenden Möglichkeiten:
   - Eingabe eines neuen Namens und Klicken auf die Schaltfläche **Neu**
   - Einfügen der Ereignissatzdaten als Text
   - Importieren der Ereignissatzdaten aus einer Datei
4. Wenn Sie einen neuen Namen eingeben und auf **Neu** klicken, werden im Fenster **Ereignissatz bearbeiten** die fünf zum Filtern von Ereignissen verwendeten Eigenschaften angezeigt.
5. Klicken Sie auf **Hinzufügen**, um dem Ereignissatz ein neues Ereignis hinzuzufügen.
6. Klicken Sie auf **Übergehen**, um ein Ereignis anzugeben, das *keinen* Alarm auslösen sollte.
7. Sie können Ereignissätze wahlweise **umbenennen**, **löschen** oder **exportieren**.

Übergehen-Bedingungen

Wenn ein Ereignisprotokolleintrag einer oder mehreren **Übergehen-Bedingungen** in einem Ereignissatz entspricht, wird *durch keinen Ereignissatz* ein Alarm ausgelöst, selbst wenn mehrere Ereignissätze einem Ereignisprotokolleintrag entsprechen. Da Übergehen-Bedingungen *alle Ereignissätze* außer Kraft setzen, ist es ratsam, nur einen Ereignissatz für alle Übergehen-Bedingungen zu definieren. Auf diese Weise müssen Sie nur an einer Stelle suchen, wenn Sie den Verdacht haben, dass eine Übergehen-Bedingung das Verhalten aller Ihrer Meldungen beeinflusst. Sie müssen den Ereignissatz mit einer Übergehen-Bedingung zunächst einer Rechner-ID zuweisen, bevor diese Bedingung alle anderen Ereignissätze, die der gleichen Rechner-ID zugewiesen wurden, außer Kraft setzen kann.

Übergehen-Bedingungen setzen nur Ereignisse des gleichen Protokolltyps außer Kraft. Wenn Sie also ein „Übergehen-Set“ für alle Übergehen-Bedingungen erstellen, muss dieses mehrmals auf die gleiche

Rechner-ID angewendet werden, nämlich *für jeden Protokolltyp einmal*. Ein Übergehen-Satz, der beispielsweise nur auf Ereignisse des Systemprotokolltyps angewendet wurde, setzt keine Ereignisbedingungen des Anwendungs- und Sicherheitsprotokolltyps außer Kraft.

1. Wählen Sie die Seite Monitor > **Ereignisprotokoll-Meldungen** aus.
2. Aktivieren Sie das Kontrollkästchen **Fehler** und wählen Sie `<All Events>` aus der Ereignissatzliste aus. Klicken Sie auf **Anwenden**, um allen ausgewählten Rechner-IDs diese Einstellung zuzuweisen. Damit weisen Sie das System an, für jeden Fehlerereignistyp eine Meldungen zu generieren. Notieren Sie den zugewiesenen Protokolltyp.
3. Erstellen Sie einen „Übergehen-Ereignissatz“, der alle Ereignisse festlegt, die Sie übergehen möchten, und weisen Sie diesen den gleichen Rechner-IDs zu. Der Protokolltyp muss dem in Schritt 2 angegebenen Protokolltyp entsprechen.

Sternchen (*) als Stellvertreterzeichen verwenden

Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.Zum Beispiel:

```
*yourFilterWord1*yourFilterWord2*
```

Dies ergäbe eine Übereinstimmung und würde einen Alarm für ein Ereignis mit der folgenden Zeichenfolge auslösen:

```
"This is a test. yourFilterWord1 as well as yourFilterWord2 are in the description."
```

Bearbeitungsereignisse exportieren und importieren

Sie können Ereignissatz-Datensätze als XML-Dateien exportieren und aus diesen importieren.

- Sie können einen vorhandenen Ereignissatz-Datensatz über das Popup-Fenster **Ereignissatz bearbeiten** in eine XML-Datei *exportieren*.
- Sie können eine Ereignissatz-XML-Datei durch Auswahl des Werts `<Import Event Set>` oder `<New Event Set>` aus der Ereignissatz-Dropdown-Liste *importieren*.

Beispiel:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<event_sets>
 <set_elements setName="Test Monitor Set" eventSetId="82096018">
   <element_data ignore="0" source="*SourceValue*"
     category="*CategoryValue*" eventId="12345"
     username="*UserValue*" description="*DescriptionValue*"/>
 </set_elements>
</event_sets>
```

Formatieren von E-Mail-Benachrichtungen für Ereignissätze

Monitor > Agent-Monitoring > Ereignisprotokoll-Meldungen > Meldungsaktionen einrichten > E-Mail formatieren

Im Fenster **E-Mail-Meldungen formatieren** wird das Format der E-Mails angegeben, die als Reaktion auf *Ereignissatz*-Meldungsbedingungen gesendet werden. Folgende Arten von Benachrichtigungs-E-Mails können über dieses Fenster formatiert werden:

- **1 – Meldung zu einem einzelnen Ereignisprotokoll** – Dieselbe Vorlage wird auf alle Ereignisprotokolltypen angewendet.
- **2 – Benachrichtigungen zu mehreren Ereignisprotokollen** – Dieselbe Vorlage wird auf alle Ereignisprotokolltypen angewendet.
- **3 – Benachrichtigung zu einem fehlenden Ereignisprotokoll** – Dieselbe Vorlage wird auf alle Ereignisprotokolltypen angewendet.

> Hinweis: Durch Ändern dieses E-Mail-Alarmformats wird das Format für alle **Ereignisprotokoll**-Benachrichtigungs-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind. Ein ● in einer nummerierten Spalte gibt an, dass eine Variable mit dem Meldungstyp, der dieser Nummer entspricht, verwendet werden kann.

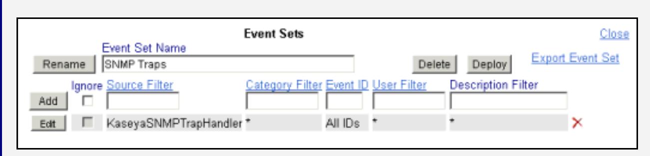
Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung	1	2	3
<um>	#at#	Alarmzeit	●	●	●
<cg>	#cg#	Ereigniskategorie	●		
<cn>	#cn#	Computername	●		
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.	●	●	●
<ed>	#ed#	Ereignisbeschreibung	●	●	
<ei>	#ei#	Ereignis-ID	●		
<es>	#es#	Ereignisquelle	●		
<et>	#et#	Ereigniszeit	●		
<eu>	#eu#	Ereignisbenutzer	●		
<ev>	#ev#	Name des Ereignissatzes	●	●	●
<gr>	#gr#	Gruppen-ID	●	●	●
<id>	#id#	Rechner-ID	●	●	●
<lt>	#lt#	Protokolltyp (Anwendung, Sicherheit, System)	●	●	●
<tp>	#tp#	Ereignistyp (Fehler, Warnung, Information, Prüfung erfolgreich, Prüfung fehlgeschlagen)	●		
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●

SNMP-Traps-Meldung

Monitor > Agent-Monitoring > SNMP-Traps-Benachrichtigungen

Die Seite **SNMP-Traps-Meldung** konfiguriert Meldungen für einen verwalteten Rechner und agiert als SNMP-Trap-Listener, wenn eine **SNMP-Trap**-Meldung erkannt wird.

Wenn **SNMP-Traps-Meldung** mit einem verwalteten Rechner verknüpft ist, wird auf diesem Rechner ein Dienst mit der Bezeichnung `Kaseya SNMP Trap Handler` gestartet. Dieser Dienst sucht nach SNMP-Trap-Meldungen, die von SNMP-fähigen Geräten auf dem gleichen LAN gesendet wurden. Wird eine SNMP-Trap-Meldung vom Dienst empfangen, wird eine SNMP-Trap-`Warning` zum `Application`-Ereignisprotokoll des verwalteten Rechners hinzugefügt. Die **Quelle** dieser `Application`-Ereignisprotokolleinträge ist immer `KaseyaSNMPTrapHandler`.

> **Hinweis:** Erstellen Sie einen Ereignissatz, der `KaseyaSNMPTrapHandler` als **Quelle** enthält. Verwenden Sie Sternchen `*` für die anderen Kriterien, wenn Sie die Ereignisse nicht weiter filtern möchten.
>
> 
>
>
> **Hinweis:** SNMP verwendet den Standard-UDP-Port 162 für SNMP-Trap-Meldungen. Achten Sie darauf, dass dieser Port offen ist, wenn eine Firewall aktiviert ist.

Ereignis-Sätze

Da die Anzahl der Ereignisse in Windows-**Ereignisprotokollen** *(siehe 618)* riesig ist, verwendet der VSA einen Datensatztyp namens **Ereignissatz**, um nach Meldungsbedingungen zu filtern. Ereignissätze enthalten eine oder mehrere **Bedingungen**. Jede Bedingung enthält Filter für verschiedene Felder in einem **Ereignisprotokolleintrag**. Die Feld sind **Quelle**, **Kategorie**, **Ereignis-ID**, **Benutzer** und **Beschreibung**. Ein **Ereignisprotokoll** *(siehe 618)*eintrag muss alle Feldfilter einer Bedingung erfüllen, um als Übereinstimmung zu gelten. Ein Feld mit einem Sternchen (*) bedeutet, dass jede Zeichenfolge, selbst eine leere Zeichenfolge, als Übereinstimmung gilt. Eine Übereinstimmung auch nur *einer* der Bedingungen in einem Ereignissatz ist ausreichend, um eine Meldung für einen Rechner auszulösen, auf den dieser Ereignissatz angewendet wurde. Weitere Hinweise zum Konfigurieren von Ereignissätzen finden Sie unter Monitor > Ereignisprotokoll-Meldungen > **Ereignissätze bearbeiten** *(siehe 320)*.

SNMP-Traps-Meldung erstellen

1. Wählen Sie die Seite Monitor > **SNMP-Traps-Meldung** aus.
2. Wählen Sie den **Ereignissatz**-Filter aus, der zum Filtern der Ereignisse verwendet wird, die Meldungen auslösen. Wählen Sie keinen Ereignissatz aus, in den *alle* SNMP-Trap-Ereignisse eingeschlossen werden sollen.
3. Aktivieren Sie das Kontrollkästchen neben der **Ereigniskategorie** `Warning`. *Keine anderen Ereigniskategorien werden von SNMP-Trap-Alarm verwendet.*

   > **Hinweis:** Rot markierte **Ereigniskategorien** (EWISFCV) geben an, dass diese Ereigniskategorien nicht vom VSA gesammelt werden. **Ereignisprotokoll-Meldungen werden auch generiert, wenn die Ereignisprotokolle nicht von VSA gesammelt werden.**

4. Geben Sie die *Häufigkeit* der Meldungsbedingung an, die zum Auslösen einer Meldung erforderlich ist:
   - **Warnen, wenn dieses Ereignis ein einziges Mal eintritt**
   - **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden>** eintritt.
   - **Warnen, wenn dieses Ereignis nicht innerhalb von <N> <Perioden>** eintritt.
   - **Zusätzliche Alarme nicht beachten für <N> <Perioden>**.
5. Klicken Sie auf die Optionsfelder **Hinzufügen** oder **Ersetzen** und anschließend auf **Anwenden**, um die ausgewählten Ereignistypmeldungen den ausgewählten Rechner-IDs zuzuweisen.

6. Klicken Sie auf **Entfernen**, um alle ereignisbasierten Meldungen von ausgewählten Rechner-IDs zu entfernen.
7. Ignorieren Sie das Feld **SNMP-Community**. *Diese Option ist noch nicht implementiert.*

Meldungsinformationen an E-Mails und Verfahren weiterleiten

> **Hinweis: SNMP-Traps-Benachrichtigung** verwendet das gleiche Fenster **E-Mail formatieren** wie Monitor > **Ereignisprotokoll-Benachrichtigungen** *(siehe 316)*.

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem

Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Protokolltyp

Der Typ des überwachten Ereignisprotokolls

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

EWISFCV

Die überwachte Ereigniskategorie

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Ereignis-Satz

Es wird `All Events` angezeigt, wenn kein *SNMP-Trap-Ereignissatz* ausgewählt wurde, was bedeutet, dass alle SNMP-Trap-Ereignisse eingeschlossen werden.

Intervall

Angabe, wie oft ein Ereignis innerhalb der festgelegten Zeitspannen eintritt. Gilt nur, wenn die Option **Warnen, wenn dieses Ereignis N> Mal innerhalb von <N> <Perioden> eintritt** aktiviert ist. Es wird `Missing` angezeigt, wenn die Option **Warnen, wenn dieses Ereignis nicht innerhalb von<N> <Perioden> eintritt** aktiviert wurde. Es wird `1` angezeigt, wenn die Option**Warnen, wenn dieses Ereignis ein einziges Mal eintritt** aktiviert wurde.

Dauer

Angabe, wie oft ein Ereignis eintreten muss, um eine Meldung auszulösen. Gilt nur, wenn die Option **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden> eintritt** oder **Warnen, wenn dieses Ereignis nicht innerhalb von <N> <Perioden> eintritt** aktiviert wurden.

Wiederherstellen

Zeigt an, wie lange gewartet werden muss, bevor neue Meldungen für die gleiche Kombination von Ereignissatz und Ereigniskategorie ausgelöst werden. Gilt nur, wenn mit **Zusätzliche Alarme übergehen für <N> <Perioden>** eine Wiederherstellungsperiode größer als Null angegeben wurde.

Monitoring zuweisen

Monitor > Agent-Monitoring > Monitor zuweisen

Auf der Seite **Monitoring zuweisen** können Sie Monitor-Set-Meldungen für verwaltete Rechner erstellen. Eine Meldung ist eine Reaktion auf eine Meldungsbedingung. Eine Meldungsbedingung liegt vor, wenn die Leistung eines Rechners vordefinierte Kriterien erfüllt oder nicht.

Monitor-Sets

Ein Monitor-Set ist ein Satz von **Zählerobjekten**, **Zählern**, **Zählerinstanzen**, **Diensten** und **Prozessen**, anhand derer die Leistung von Rechnern überwacht werden kann. In der Regel wird jedem/jeder **Objekt/Instanz/Zähler** *(siehe 620)*, Dienst oder Prozess in einem Monitor-Set ein Schwellenwert zugewiesen. Sie können Alarme festlegen, die ausgelöst werden, wenn einer der Schwellenwerte im Monitor-Set überschritten wird. Ein Monitor-Set sollte als eine logische Gruppierung von Faktoren, die überwacht werden sollen, verstanden werden. Eine solche logische Gruppierung könnte beispielsweise die Überwachung alle zum Ausführen eines Exchange Server erforderlichen Zähler und Dienste sein. Sie können jedem Rechner, auf dem das Betriebssystem Windows 2000 oder höher ausgeführt wird, ein Monitor-Set zuweisen.

Das allgemeine Verfahren zum Arbeiten mit Monitor-Sets ist wie folgt:

1. Sie können die Objekte, Instanzen und Zähler von Monitor-Sets über **Monitorlisten** *(siehe 264)* wahlweise auch manuell aktualisieren und prüfen.
2. Erstellen und pflegen Sie Monitor-Sets über Monitor > **Monitor-Sets** *(siehe 267)*.
3. Weisen Sie Monitor-Sets über Monitor > **Monitor zuweisen** *(siehe 327)* bestimmten Rechner-IDs zu.
4. Wahlweise können Sie Standard-Monitor-Sets als *individualisierte Monitor-Sets* anpassen.
5. Die wahlweise Anpassung von Standard-Monitor-Sets erfolgt über *Auto-Lernen*.
6. Überprüfen Sie Monitor-Sets über folgende Befehle:
   - Monitor > **Monitor-Protokoll** *(siehe 333)*
   - Monitor > **Live Counter** *(siehe 263)*
   - Monitor > Dashboard > **Netzwerkstatus** *(siehe 255)*
   - Monitor > Dashboard > **Gruppenalarmstatus** *(siehe 256)*
   - Monitor > Dashboard > **Monitor-Set-Status** *(siehe 256)*
   - Info Center > Reporting > Berichte > Monitor > Monitor-Set-Bericht
   - Info Center > Reporting > Berichte > Monitor > Monitor-Aktionsprotokoll

> **Hinweis:** An einem Monitor-Set vorgenommene Änderungen wirken sich innerhalb weniger Minuten nach der Änderung auf alle Rechner-IDs aus, denen dieses Monitor-Set zugewiesen ist.

Individualisierte Monitor-Sets

Sie können die Monitor-Set-Einstellungen für einen einzelnen Rechner *individualisieren*.

1. Wählen Sie mit Monitor > **Monitor zuweisen** ein *Standard*-Monitor-Set aus der `<Select Monitor Set>`-Dropdown-Liste aus.
2. Weisen Sie dieses Standard-Monitor-Set einer Rechner-ID zu. Der Name des Monitor-Sets wird in der Spalte **Monitor-Set**angezeigt.
3. Klicken Sie auf das individualisierte Monitor-Set-Symbol in der Spalte **Monitor-Set**, um die gleichen Optionen wie beim Definieren eines **Standard-Monitor-Sets** *(siehe 267)* anzuzeigen. *Bei einem individualisierten SNMP-Set wird dem Namen des SNMP-Sets ein (IND) Präfix vorangestellt.*
4. Sie können den Namen oder die Beschreibung des individualisierten Monitor-Sets auf Wunsch ändern. Klicken Sie anschließend auf **Speichern**. Durch Bereitstellung eines eindeutigen Namens und einer Beschreibung kann ein individualisiertes Monitor-Set in Berichten und Protokolldateien identifiziert werden.
5. Nehmen Sie Änderungen an den Kontrolleinstellungen des individualisierten Monitor-Sets vor und klicken Sie auf **Einspeichern**. Änderungen gelten nur für den einzelnen Rechner, dem das individualisierte Monitor-Set zugewiesen ist.

> **Hinweis:** Änderungen an einem Standard-Monitor-Set haben keine Auswirkungen auf die individualisierten Monitor-Sets, die davon kopiert wurden.

Auto-Lernen-Alarmschwellenwerte für Monitor-Sets

Sie können **Auto-Lernen**-Alarmschwellenwerte für jedes Standard-Monitor-Set aktivieren, das Sie ausgewählten Rechner-IDs zuweisen. Damit werden Alarmschwellenwerte basierend auf tatsächlichen Leistungsdaten auf die einzelnen Rechner abgestimmt.

Jeder zugewiesene Rechner generiert Leistungsdaten für die angegebene Zeitspanne. Während dieser Zeitspanne werden keine Alarme ausgelöst. Am Ende der Auto-Lernen-Sitzung wird der Alarmschwellenwert für jeden zugewiesenen Rechner basierend auf der tatsächlichen Leistung des Rechners automatisch abgestimmt. Sie können die Alarmschwellenwerte, die durch **Auto-Lernen** berechnet wurden, manuell anpassen oder eine weitere **Auto-Lernen**-Sitzung ausführen. **Auto-Lernen** kann nicht mit individualisierten Monitor-Sets verwendet werden.

So wenden Sie **Auto-Lernen**-Einstellungen auf ausgewählte Rechner-IDs an:

1. Wählen Sie mit Monitor > **Monitor zuweisen** ein *Standard*-Monitor-Set aus der `<Select Monitor Set>`-Dropdown-Liste aus.
2. Klicken Sie auf **Auto-Lernen**, um das Popup-Fenster **Auto-Lernen** *(siehe 332)* einzublenden. Definieren Sie mithilfe eines Assistenten die Parameter, die zum Berechnen der Alarmschwellenwerte verwendet werden.
3. Weisen Sie dieses Standard-Monitor-Set, das durch Ihre Auto-Lernen-Parameter abgeändert wurde, ausgewählten Rechner-IDs zu.

> **Hinweis:** Sie können Auto-Lernen-Einstellungen keinem Monitor-Set zuweisen, das bereits einer Rechner-ID zugewiesen wurde. Löschen Sie gegebenenfalls die vorhandene Zuweisung des Monitor-Sets für die Rechner-ID und führen Sie dann die Schritte 1 bis 3 oben aus.

Sobald Auto-Lernen auf eine Rechner-ID angewendet und für die vorgegebene Zeitspanne ausgeführt wurde, können Sie für eine bestimmte Rechner-ID auf das Auto-Lernen-überschreiben-Symbol klicken und die berechneten Alarmschwellenwerte manuell anpassen. Sie können auch Auto-Lernen in einer neuen Sitzung unter Verwendung der tatsächlichen Leistungsdaten erneut ausführen, um die Alarmschwellenwerte neu zu berechnen.

So erstellen Sie eine Monitor-Set-Meldung:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:

- **A**larm erstellen
- **T**icket erstellen
- **S**kript ausführen
- **E**-Mail-Empfänger

2. Legen Sie weitere E-Mail-Parameter fest.
3. Wählen Sie das Monitor-Set aus, das hinzugefügt oder ersetzt werden soll.
4. Markieren Sie die Rechner-IDs, auf die der Alarm angewendet werden soll.
5. Klicken Sie auf die Schaltfläche **Apply**.

So brechen Sie eine Monitor-Set-Meldung ab:

1. Aktivieren Sie das Kontrollkästchen für die Rechner-ID.
2. Klicken Sie auf die Schaltfläche **Löschen**.

   Die neben der Rechner-ID aufgeführten Meldungsinformationen werden gelöscht.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitor-Meldungs-E-Mails können gesendet und formatiert werden:

- Monitoring des Schwellenwertalarms
- Monitoring des Trendschwellenwertalarms
- Benachrichtigung über Monitoring des Endalarmstatus

> **Hinweis:** Durch Ändern des E-Mail-Alarm-Formats wird das Format für *alle* Monitor-Set- und SNMP-Set-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	**Innerhalb eines Verfahrens**	**Beschreibung**
<ad>	#ad#	Alarmdauer
<ao>	#ao#	Alarm-Betreiber
<um>	#at#	Alarmzeit
<av>	#av#	Alarmschwellenwert
<cg>	#cg#	Ereigniskategorie
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<dv>	#dv#	SNMP-Gerätename
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<ln>	#ln#	Monitoring-Protokoll-Objektname
<lo>	#lo#	Monitoring-Protokoll-Objekttyp: Zähler, Prozess, Objekt
<lv>	#lv#	Monitoring-Protokollwert

<mn>	#mn#	Monitor-Set-Name
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

(Filter anwenden)

Geben Sie Text in das Filter-Bearbeitungsfeld ein und klicken Sie auf das Trichtersymbol, um die Filterung auf die in **Monitor-Set auswählen** angezeigte Dropdown-Liste anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in dem Satznamen gefunden wird.

Monitor-Set auswählen

Wählen Sie Monitor-Sets aus der Liste **Monitor-Set auswählen** aus und klicken Sie auf **Anwenden**, um das Monitor-Set allen ausgewählten Rechner-IDs zuzuweisen. Sie können einer Rechner-ID mehr als ein Monitor-Set zuweisen. Das Hinzufügen oder Bearbeiten von Monitor-Sets erfolgt über Monitor >

Monitor-Sets *(siehe 267)*.

> **Hinweis:** Beispiel-Monitor-Sets werden nicht in der Dropdown-Liste **Monitor zuweisen** *(siehe 327)* > **Monitor-Set auswählen** angezeigt. Erstellen Sie eine Kopie des Beispiel-Monitor-Sets, indem Sie das Beispielset in **Monitor-Sets** *(siehe 267)* auswählen und auf die Schaltfläche **Speichern unter** klicken. Ihre Kopie des Beispiel-Monitor-Sets wird in der Dropdown-Liste angezeigt. In einem **SaaS** *(siehe 631)*-basierten VSA sind die Schaltflächen **Speichern** und **Speichern unter** verfügbar. Sie können Änderungen am Beispielsatz vornehmen und diesen sofort verwenden, da er nicht aktualisiert wird.

Monitor-Set hinzufügen

Wenn ein Monitor-Set Rechner-IDs zugewiesen wird, wird es zu der Liste der gegenwärtig diesen Rechner-IDs zugewiesenen Monitor-Sets hinzugefügt.

Monitor-Set ersetzen

Wenn ein Monitor-Set Rechner-IDs zugewiesen wird, ersetzt es alle gegenwärtig diesen Rechner-IDs zugewiesenen Monitor-Sets.

Anwenden

Wendet das ausgewählte Monitor-Set auf die markierten Rechner-IDs an.

Löschen

Löscht die Zuweisung eines ausgewählten Monitor-Sets auf ausgewählten Rechner-IDs.

Alle löschen

Löscht alle Monitor-Sets, die ausgewählten Rechner-IDs zugewiesen sind.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Monitor-Sets

Zeigt eine Liste aller Monitor-Sets an, die Rechner-IDs zugewiesen sind.

– **Bearbeiten** – Diese Option wird immer neben einem Monitor-Set angezeigt. Klicken Sie auf

dieses Symbol, um Kopfzeilenparameter einzustellen, die mit denjenigen der ausgewählten Rechner-ID übereinstimmen.

– **Auto-Lernen-Werte überschreiben** – Diese Option wird angezeigt, wenn Auto-Lernen auf dieses standardmäßige Monitor-Set angewendet wurde. Klicken Sie auf dieses Symbol, um die tatsächlichen Werte anzuzeigen oder zu ändern, die mit **Auto-Lernen** *(siehe 332)* für dieses Monitor-Set auf dieser Rechner-ID berechnet wurden.

– **Individualisiertes Monitor-Set** – Diese Option wird angezeigt, wenn Auto-Lernen *nicht* auf dieses standardmäßige Monitor-Set angewendet wurde. Klicken Sie auf dieses Symbol, um ein **standardmäßiges Monitor-Set** *(siehe 267)* zu erstellen bzw. Änderungen an einer Kopie davon vorzunehmen, die spezifisch (individualisiert) für diese Rechner-ID ist. *Bei einem individualisierten Monitor-Set wird dem Namen des Monitor-Sets ein (IND) Präfix vorangestellt.*

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Auto-Lernen – Monitor-Sets

Monitor > Agent-Monitoring > Monitor zuweisen > Auto-Lernen

Über das Fenster **Auto-Lernen-Alarmschwellenwerte** werden die Auto-Lernen-Alarmschwellenwerte für Monitor-Sets gepflegt.

Sie können **Auto-Lernen**-Alarmschwellenwerte für jedes Standard-Monitor-Set aktivieren, das Sie ausgewählten Rechner-IDs zuweisen. Damit werden Alarmschwellenwerte basierend auf tatsächlichen Leistungsdaten auf die einzelnen Rechner abgestimmt.

Jeder zugewiesene Rechner generiert Leistungsdaten für die angegebene Zeitspanne. Während dieser Zeitspanne werden keine Alarme ausgelöst. Am Ende der Auto-Lernen-Sitzung wird der Alarmschwellenwert für jeden zugewiesenen Rechner basierend auf der tatsächlichen Leistung des Rechners automatisch abgestimmt. Sie können die Alarmschwellenwerte, die durch **Auto-Lernen** berechnet wurden, manuell anpassen oder eine weitere **Auto-Lernen**-Sitzung ausführen. **Auto-Lernen** kann nicht mit individualisierten Monitor-Sets verwendet werden.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Bearbeiten

Es wird eine Liste der **Objekte/Instanzen/Zähler** *(siehe 620)* für das ausgewählte Monitor-Set angezeigt, das Sie für Auto-Lernen konfigurieren möchten. Klicken Sie auf das Bearbeitungssymbol, um einen Assistenten aufzurufen, der Sie durch die drei Schritte zum Bearbeiten von Auto-Lernen-Alarmschwellenwerten führt.

1. Aktivieren Sie Auto-Lernen für diese Objekt/Zähler/Instanz-Kombination, indem Sie `Yes - Include` auswählen. Wenn `No - Do not include` ausgewählt ist, sind keine weiteren Auswahlen in diesem Assistenten zutreffend.

- **Zeitspanne** – Geben Sie an, wie lange Leistungsdaten erfasst und zur automatischen Berechnung der Alarmschwellenwerte verwendet werden sollen. Während dieser Zeitspanne werden keine Alarme gemeldet.

2. Zeigt das **Objekt**, den **Zähler** und gegebenenfalls die **Instanz** des zu ändernden Alarmschwellenwerts an. Diese Optionen können nicht geändert werden.
3. Geben Sie Parameter für die Wertberechnung ein.
   - **Berechnung** – Geben Sie einen Parameter für die Wertberechnung ein. Mögliche Optionen sind `MIN`, `MAX` oder `AVG`. Bei Auswahl von `MAX` wird beispielsweise der maximale Wert berechnet, der für eine Objekt/Zähler/Instanz-Kombination während der oben angegebenen **Zeitspanne** erfasst wurde.
   - **% Anstieg** – Fügen Sie diesen Anstieg zu dem oben berechneten **Berechnung**swert hinzu, wobei der **Berechnung**swert 100% darstellt. Der resultierende Wert stellt den Alarmschwellenwert dar.
   - **Minimum** – Legen Sie einen Mindestwert für den Alarmschwellenwert fest. Dieser Wert wird automatisch als *zwei Standardabweichungen unter* dem berechneten **Berechnung**swert berechnet, doch dieser Wert kann manuell überschrieben werden.
   - **Maximum** – Legen Sie einen Maximalwert für den Alarmschwellenwert fest. Dieser Wert wird automatisch als *zwei Standardabweichungen über* dem berechneten **Berechnung**swert berechnet, doch dieser Wert kann manuell überschrieben werden.

Hinweis: Sobald Auto-Lernen auf eine Rechner-ID angewendet und für die vorgegebene Zeitspanne ausgeführt wurde, können Sie für eine bestimmte Rechner-ID auf das Auto-Lernen-Überschreiben-Symbol klicken und die berechneten Alarmschwellenwerte manuell anpassen. Sie können auch Auto-Lernen in einer neuen Sitzung unter Verwendung der tatsächlichen Leistungsdaten erneut ausführen, um die Alarmschwellenwerte neu zu berechnen.

Weiter

Geht zu nächsten Seite im Assistenten.

Zurück

Geht zu vorherigen Seite im Assistenten.

Speichern

Speichert Änderungen an einem Datensatz.

Abbrechen

Ignoriert die vorgenommen Änderungen und kehrt zur Liste der Datensätze zurück.

Monitor-Protokoll

Monitor > Agent-Monitoring > Monitor-Protokoll

- Durch Klicken auf das Monitor-Protokoll-Symbol neben einem einzelnen Alarm für eine bestimmte Rechner-ID im Dashlet Monitor-Set-Status *(siehe 256)* der Seite Dashboard-Liste werden die gleichen Informationen wie ein Popup-Fenster angezeigt.

Auf der Seite **Monitor-Protokoll** werden die Agent-Monitoring-Objektprotokolle als Diagramm und in tabellarischer Form angezeigt.

Rechner-ID.Gruppen-ID

Klicken Sie auf einen Rechner-ID-Link, um die Protokolldaten für alle Monitor-Sets anzuzeigen, die dieser Rechner-ID zugewiesen sind. Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert

auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, für die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen. Wenn keine Rechner-IDs angezeigt werden, weisen Sie mit Monitor > **Monitor zuweisen** *(siehe 327)* Monitor-Sets den Rechner-IDs zu.

Monitoring-Objekt zur Anzeige von Informationen auswählen

Auf dieser Seite wird eine Liste von Monitoring-Objekten angezeigt, die der ausgewählten Rechner-ID zugewiesen wurden.

Ansicht

Wählen Sie ein Zählerobjekt aus, indem Sie auf den Link **Ansicht** klicken. Die ausgewählte Zeile wird **fettgedruckt** dargestellt. Eine ausgewählte Zeile wird entweder als Diagramm oder als Tabelle dargestellt.

> **Hinweis:** Wenn ein Kontrollobjekt nicht als Diagramm dargestellt werden kann, ist nur die Tabellenansicht verfügbar.

Erweiterungssymbol

Klicken Sie auf das Erweiterungssymbol ⊞, um weitere Details zu einem Monitoring-Objekt anzuzeigen.

Daten aktualisieren

Klicken Sie auf das Aktualisieren-Symbol, um die Daten zu aktualisieren, wenn keine Werte angezeigt werden. Diese Option steht zur Verfügung, wenn Sie beim Monitoring keine Reaktion erhalten.

Falls Ihr Monitor keine Protokollwerte anzeigt, überprüfen Sie Folgendes:

1. Prüfen Sie das Intervall des Zählerobjekts. Sobald ein Monitor-Set bereitgestellt wurde, geben die Zähler Werte an das Monitor-Protokoll, die während des angegebenen Abfrageintervalls erfasst wurden. Warten Sie das Ende des Abfrageintervalls plus das Agent-Check-in-Intervall ab, bevor Sie auf die ersten zurückgegebenen Werte prüfen.
2. Falls keine Werte zurückgegeben wurden, prüfen Sie die **ZählerSchwellenwerte** *(siehe 271)* auf die Kontrollzähler-Werte. Falls keine Werte auf dem überwachten Rechner oder Gerät den Erfassungsschwellenwert erfüllen, werden diese nicht in das Monitor-Protokoll aufgenommen.

Wenn ein Monitor nicht reagiert, erscheint im Protokoll die Meldung `Monitor Not Responding`. Es kann verschiedene Gründe geben, weshalb ein Monitor nicht reagiert:

- **Zähler –** Falls Ihr Monitor-Set einen Zähler beinhaltet, der auf einem verwalteten Rechner nicht existiert, erscheint im Protokoll `Not Responding`. Sie können das Monitoring von Zählern für einen bestimmten Rechner auf zweierlei Weisen auf Fehler prüfen:
  - Scannen Sie mit Monitor > **Listen nach Scan aktualisieren** *(siehe 266)* alle Monitorzähler und -dienste *für diese Rechner-ID*.
  - Stellen Sie eine Verbindung mit dem durch diesen Agents verwalteten Rechner her, indem Sie den Befehl **Ausführen** im **Start**-Menü auswählen, `perfmon.exe` eingeben, auf **OK** klicken, ein neues **Zählerprotokoll** erstellen und auf das Vorhandensein von Zähler-Objekten/Zählern/Instanzen prüfen, die nicht antworten.
  - Ein Zählerwert von -008 in den Kontrollprotokollen gibt an, dass der Monitorset keine Daten zurückgibt. Überprüfen Sie, dass der `Performance Logs & Alerts`-Dienst in Windows ausgeführt wird. Dies ist eine Voraussetzung für die Überwachung der Leistungszähler.
- **Dienste –** Falls Ihr Monitor-Set einen Dienst beinhaltet, der auf einem verwalteten Rechner nicht existiert, erscheint im Protokoll `Service Does Not Exist`.
- **Prozesse –** Falls Ihr Monitor-Set einen Prozess beinhaltet, der auf einem verwalteten Rechner nicht existiert, erscheint im Protokoll `Process Stopped`.

- **Berechtigungen** – Achten Sie darauf, dass die Zugriffsberechtigungen für das **Arbeitsverzeichnis** *(siehe 72)* des Agents auf vollen Zugriff für `SYSTEM` und `NETWORK SERVICE` eingestellt sind. Hier kann es Probleme geben, wenn das Arbeitsverzeichnis des Agents in den Verzeichnissen `c:\program files\` oder `c:\windows` abgelegt wird. Hiervon ist abzuraten, da für diese Verzeichnisse vom Betriebssystem spezielle Zugriffsberechtigungen festgelegt werden.

Typ

Der Typ des Monitorobjekts: Zähler, Prozess oder Dienst

Name des Monitor-Sets

Der Name des Monitor-Sets

Objektname

Der Name des Monitorobjekts

Letzter Wert

Der letzte gemeldete Wert

Balkendiagramm/Tabelle

Aktivieren Sie das Optionsfeld **Balkendiagramm** oder **Tabelle**, um die Daten im gewünschten Format anzuzeigen. Nur Monitor-Objekte des Typs **Zähler** können als Balkendiagramm dargestellt werden.

- In einem Balkendiagramm werden die letzten 2000 Datenpunkte für die Abfrageintervallfrequenz dargestellt. Der Hintergrund des Diagramms ist rot für Alarmschwellenwert, gelb für Warnungsschwellenwert und grün, wenn kein Alarm.
- In den Tabellenprotokolldaten werden die aktuellen Werte zuerst aufgeführt. Außerdem werden Alarm- und Warnungssymbole für Protokolldaten angezeigt, die in diese Schwellenwerte fallen. Weitere Informationen finden Sie unter **Monitor-Set definieren** *(siehe 278)*.

Startdatum/Letzte anzeigen

Anzeigen der Protokolldaten für die letzte Anzahl der Intervalle, die seit dem angegebenen Datum ausgewählt wurden. Ist kein Datum angegeben, wird das aktuelle Datum verwendet. Wenn Sie beispielsweise **Letzte 500 Minuten** auswählen, stellt jeder Balken in dem Diagramm 1 Minute dar.

Ansicht speichern

Sie können den Wert **Letzte anzeigen** für ein bestimmtes Monitor-Objekt speichern.

Protokollzeilen pro Seite

Diese Felder werden nur im **Tabellen**format angezeigt. Wählen Sie die Anzahl der Zeilen aus, die pro Seite angezeigt werden sollen.

Wert über/unter anzeigen

Diese Felder werden nur im **Tabellen**format angezeigt. Filtern Sie die Tabellenzeilen, indem Sie Protokolldaten, die über oder unter dem angegebenen Wert liegen, herausfiltern.

Aktualisieren

Klicken Sie auf die Schaltfläche „Aktualisieren“, nachdem Sie Filteränderungen vorgenommen haben.

Seite wählen

Diese Schaltfläche wird nur angezeigt, wenn das **Tabellen**format ausgewählt ist. Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Systemprüfung

Monitor > Externes Monitoring > Systemprüfung

Der VSA kann auch Rechner überwachen, *auf denen kein Agent installiert ist*. Diese Funktion wird auf einer einzelnen Seite namens **Systemprüfung** durchgeführt. Rechner ohne einen Agent werden als **externe Systeme** bezeichnet. Einem Rechner mit einem Agent wird die Aufgabe zugewiesen, die Systemprüfung auf dem externen System durchzuführen. Durch eine Systemprüfung wird normalerweise festgestellt, ob ein externes System verfügbar ist oder nicht. Es gibt folgende Arten von Systemprüfungen: Webserver, DNSserver, Portverbindung, Ping und benutzerdefiniert.

So erstellen Sie eine Systemüberwachungsmeldung:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
2. Legen Sie weitere E-Mail-Parameter fest.
3. Legen Sie weitere Parameter zur Systemprüfung fest. Sie können mehrere Systeme mit der gleichen Rechner-ID prüfen.
4. Markieren Sie die Rechner-IDs, auf die der Alarm angewendet werden soll.
5. Klicken Sie auf die Schaltfläche **Apply**.

So brechen Sie eine Systemprüfungsmeldung ab:

1. Aktivieren Sie das Kontrollkästchen für die Rechner-ID.
2. Klicken Sie auf die Schaltfläche **Löschen**.

   Die neben der Rechner-ID aufgeführten Meldungsinformationen werden gelöscht.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Systemprüfungs-E-Mails können gesendet und formatiert werden:

- Meldung bei Systemprüfung

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<um>	#at#	Alarmzeit
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<p1>	#p1#	Geprüfte Adresse
<p2>	#p2#	Weiterer Parameter
<sc>	#sc#	Typ der Systemprüfung

<scn>	#scn#	Benutzerdefinierter Name der Systemprüfung
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Anwenden

Klicken Sie auf **Anwenden**, um die Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Informationen korrekt angewendet wurden.

Löschen

Klicken Sie auf **Löschen**, um alle Parametereinstellungen von ausgewählten Rechner-IDs zu entfernen.

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Parameter zur Systemprüfung

Wählen Sie einen Systemprüfungstyp aus:

- **Webserver** – Geben Sie eine URL ein, um in einem festgelegten Zeitintervall zu pollen.
- **DNS-Server** – Geben Sie eine DNS-Adresse ein, entweder einen Namen oder eine IP-Adresse, um in einem festgelegten Zeitintervall zu pollen.
- **Portverbindung** – Geben Sie eine Adresse, entweder einen Namen oder eine IP-Adresse, sowie eine Portnummer ein, mit der Sie in einem festgelegten Zeitintervall eine Verbindung herstellen möchten.
- **Ping** – Geben Sie eine Adresse ein, entweder einen Namen oder eine IP-Adresse, die Sie in einem festgelegten Zeitintervall anpingen möchten.

> **Hinweis:** Schließen Sie nicht den Schemanamen einer URL in die Adresse ein, die Sie anpingen möchten. Geben Sie beispielsweise nicht `http://www.google.com` ein. Geben Sie stattdessen `www.google.com` ein.

- **Benutzerdefiniert** – Geben Sie einen Pfad zu einem benutzerdefinierten Programm und einer Ausgabedatei ein, die Sie in einem festgelegten Zeitintervall ausführen möchten.
  - **Programm, Parameter und Ausgabedatei** – Geben Sie den Programmpfad ein. Geben Sie wahlweise einen Parameter ein, mit dem eine Ausgabedatei erstellt wird, falls zutreffend. Zum Beispiel: `c:\temp\customcheck.bat > c:\temp\mytest.out`.
  - **Pfad und Name der Ausgabedatei** – Geben Sie den Namen und Pfad der erstellten Ausgabedatei ein. Zum Beispiel: `c:\temp\mytest.out`.
  - **Alarm, wenn die Ausgabedatei enthält/nicht enthält** – Alarm, wenn die Ausgabedatei den festgelegten Text enthält/nicht enthält. Zum Beispiel: `Hello World`.

Die folgenden optionalen Parameter werden für alle Arten von Systemprüfungen angezeigt:

- **Alle N Perioden** – Geben Sie ein, wie oft diese Aufgabe in jeder Zeitperiode ausgeführt werden soll.
- **Hinzufügen** – Fügen Sie diese Systemprüfung zu den ausgewählten Rechner-IDs hinzu.
- **Ersetzen** – Fügen Sie diese Systemprüfung zu den ausgewählten Rechner-IDs hinzu und entfernen Sie alle bestehenden Systemprüfungen.
- **Entfernen** – Entfernen Sie diese Systemprüfung von den ausgewählten Rechner-IDs.
- **Benutzerdefinierter Name** – Geben Sie einen benutzerdefinierten Namen ein, der in Alarmnachrichten und formatierten E-Mails angezeigt wird.
- **Alarm nur auslösen, wenn der Dienst weiterhin für N Perioden nicht antwortet** – Unterdrückt das Auslösen einer Systemprüfungsmeldung für eine festgelegte Anzahl von Perioden, nachdem das Problem erstmals *festgestellt* wurde, falls N größer als Null. Dies verhindert das Auslösen eines Alarms für ein temporäres Problem.
- **Zusätzliche Alarme übergehen für N Perioden** – Unterdrückt das Auslösen weiterer Alarme für die gleiche Systemprüfung für eine festgelegte Anzahl von Perioden, nachdem das Problem erstmals *gemeldet* wurde, falls N größer als Null. Dadurch wird verhindert, dass mehrere Alarme für das gleiche Problem gemeldet werden.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Löschen

Klicken Sie auf das Löschen-Symbol , um eine Systemprüfung zu löschen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Typ

Der Typ der Systemprüfung:

- Webserver
- DNS-Server
- Portverbindung
- Ping
- Benutzerdefiniert

Intervall

Das Intervall, während dessen die Systemprüfung stattfinden soll

Dauer

Die Anzahl der Perioden, während derer die Systemprüfungsmeldung unterdrückt wird, nachdem das Problem erstmals *festgestellt* wurde. Dies verhindert das Auslösen eines Alarms für ein temporäres Problem.

Zurücksetzen

Angabe, wie lange weitere Meldungsbedingungen unterdrückt werden sollen, nachdem die erste gemeldet wurde. Dadurch wird verhindert, dass mehrere Alarme für das gleiche Problem erzeugt werden.

SNMP zuordnen

Monitor > SNMP-Monitoring > SNMP zuweisen

Über die Seite **SNMP zuweisen** werden SNMP-Meldungen für SNMP-Geräte erstellt, die bei einem **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* ermittelt werden. Eine **Meldung** *(siehe 621)* ist eine Reaktion auf eine Meldungsbedingung.

Ein SNMP-Set ist ein Satz von MIB-Objekten, mit denen Sie die Leistung **SNMP-aktivierter Netzwerkgeräte** *(siehe 629)* überwachen können. Das SNMP-Protokoll wird benutzt, weil auf diesen Geräten kein Agent installiert werden kann. Sie können jedem Leistungsobjekt in einem SNMP-Set Alarmschwellenwerte zuweisen. Wenn Sie dem SNMP-Set einem Gerät zuweisen, werden Sie benachrichtigt, wenn der Alarmschwellenwert überschritten wird. Anhand der folgenden Methoden können Sie SNMP-Sets definieren und Rechner-IDs zuweisen.

- **SNMP-Schnellsets** – Erstellt ein gerätespezifisches SNMP-Set basierend auf den beim einem LAN-Watch auf diesem Gerät ermittelten Objekten und weist es zu. **SNMP-Schnellsets** *(siehe 629)* sind die einfachste Methode, SNMP-Monitoring auf einem Gerät zu implementieren.
- **SNMP-Standardsets** – Hierbei handelt es sich für gewöhnlich um generische SNMP-Sets, die auf mehrere Geräte angewendet und auf diesen gepflegt werden. Nachdem ein Schnellset erstellt wurde, kann dieses als ein Standardset gepflegt werden.
- **Individualisierte SNMP-Sets** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann manuell angepasst wurden.
- **SNMP-Auto-Lernen** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann automatisch über Auto-Lernen angepasst wurden.
- **SNMP-Typen** – Damit bezeichnet man eine Methode, SNMP-Standardsets, basierend auf dem während eines LAN-Watch festgestellten **SNMP-Typ** *(siehe 630)*, automatisch Geräten zuzuweisen.

In der Regel verwenden Sie das folgende Verfahren, um SNMP-Sets zu konfigurieren und Geräten zuzuweisen.

1. Ermitteln Sie SNMP-Geräte über Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor >**SNMP zuweisen** *(siehe 340)* den ermittelten Geräten zu. Diese können SNMP-Schnellsets, -Standardsets, individualisierte oder Auto-Lernen-Sets einschließen.
3. Zeigen Sie SNMP-Alarme mit Monitor > **SNMP-Protokoll** *(siehe 349)* oder **Dashboard-Liste** *(siehe 251)* an.

Die folgenden zusätzlichen SNMP-Funktionen stehen zur Verfügung und können in beliebiger Reihenfolge verwendet werden.

- Überprüfen Sie wahlweise die Liste aller importierten SNMP-Objekte mit Monitor > **Monitorlisten** *(siehe 264)*.
- Die Pflege von SNMP-Sets kann wahlweise mit Monitor > **SNMP-Sets** *(siehe 276)* erfolgen.
- Mit Monitor > **SNMP-Objekt hinzufügen** *(siehe 281)* können Sie wahlweise ein SNMP-Objekt hinzufügen.
- Mit Monitor > **SNMP-Typ konfigurieren** *(siehe 352)* können Sie wahlweise manuell einen SNMP-Typ einem SNMP-Gerät zuweisen.
- Mit Monitor > **SNMP-Werte einstellen** *(siehe 350)* können Sie wahlweise Werte auf SNMP-Geräte schreiben.

Individualisierte SNMP-Sets

Sie können die SNMP-Set-Einstellungen für einen einzelnen Rechner *individualisieren*.

1. Wählen Sie ein *Standard*-SNMP-Set aus der `<Select Monitor Set>`-Dropdown-Liste aus.
2. Weisen Sie dieses Standard-SNMP-Set einem SNMP-Gerät zu. Der Name des SNMP-Sets wird in der Spalte **SNMP-Info/SNMP-Set** angezeigt.

3. Klicken Sie auf das individualisierte SNMP-Set-Symbol in der Spalte **SNMP-Info/SNMP-Set**, um die gleichen Optionen wie beim Definieren eines **Standard-SNMP-Sets** *(siehe 276)* anzuzeigen. *Bei einem individualisierten SNMP-Set wird dem Namen des SNMP-Sets ein (IND) Präfix vorangestellt.*
4. Nehmen Sie Änderungen an dem neuen individualisierten SNMP-Set vor. Diese Änderungen gelten nur für das einzelne SNMP-Gerät, dem dieses SNMP-Set zugewiesen wurde.

> **Hinweis:** Änderungen an einem SNMP-Set haben keine Auswirkungen auf die individualisierten SNMP-Sets, die davon kopiert wurden.

Auto-Lernen-Alarmschwellenwerte für SNMP-Sets

Sie können **Auto-Lernen**-Alarmschwellenwerte für jedes beliebige SNMP-Set bzw. -Schnellset aktivieren, das Sie ausgewählten SNMP-Geräten zuweisen. Damit werden Alarmschwellenwerte basierend auf tatsächlichen Leistungsdaten auf die einzelnen SNMP-Geräte abgestimmt.

Jedes zugewiesene SNMP-Gerät generiert Leistungsdaten für die angegebene Zeitspanne. Während dieser Zeitspanne werden keine Alarme ausgelöst. Am Ende der **Auto-Lernen**-Sitzung wird der Alarmschwellenwert für jedes zugewiesene SNMP-Gerät basierend auf der tatsächlichen Leistung des SNMP-Geräts automatisch abgestimmt. Sie können die Alarmschwellenwerte, die durch **Auto-Lernen** berechnet wurden, manuell anpassen oder eine weitere **Auto-Lernen**-Sitzung ausführen. **Auto-Lernen** kann nicht mit individualisierten SNMP-Sets verwendet werden

So wenden Sie **Auto-Lernen**-Einstellungen auf ausgewählte SNMP-Geräte an:

1. Wählen Sie ein *Standard*-SNMP-Set aus der `<Select SNMP Set>`-Dropdown-Liste aus. Sie können auch auf das Bearbeitungssymbol eines SNMP-Sets klicken, der bereits einem Gerät zugeordnet ist, um den Identifikator in die `<Select SNMP Set>`-Dropdown-Liste zu übertragen.
2. Klicken Sie auf **Auto-Lernen**, um das Popup-Fenster **Auto-Lernen** *(siehe 332)* einzublenden. Definieren Sie mithilfe eines Assistenten die Parameter, die zum Berechnen der Alarmschwellenwerte verwendet werden.
3. Weisen Sie dieses Standard-SNMP-Set, das durch Ihre **Auto-Lernen**-Parameter abgeändert wurde, ausgewählten SNMP-Geräten zu, falls dies noch nicht geschehen ist.

Sobald **Auto-Lernen** auf eine Rechner-ID angewendet und für die vorgegebene Zeitspanne ausgeführt wurde, können Sie für ein bestimmtes SNMP-Gerät auf das Auto-Lernen-überschreiben-Symbol klicken und die berechneten Alarmschwellenwerte manuell anpassen. Sie können auch **Auto-Lernen** in einer neuen Sitzung unter Verwendung der tatsächlichen Leistungsdaten erneut ausführen, um die Alarmschwellenwerte neu zu berechnen.

Schnellsets

Auf der Seite **SNMP-Info** wird eine Liste der MIB-Objekte angezeigt, die von dem jeweils ausgewählten SNMP-Gerät bereitgestellt werden. Diese MIB-Objekte werden durch Ausführen eines beschränkten SNMP-Durchlaufs auf allen ermittelten SNMP-Geräten ermittelt, wann immer ein **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* stattfindet. Sie können die Liste der ermittelten MIB-Objekte verwenden, um sofort ein gerätespezifisches SNMP-Set mit der Bezeichnung **Schnellset** zu erstellen und auf das Gerät anzuwenden. Schnellsets entsprechen nach der Erstellung den Standardsets. Sie werden in Ihrem privaten Ordner in Monitor > **SNMP-Sets** und in der Dropdown-Liste in Monitor > **SNMP zuweisen** angezeigt. Ein `(QS)`-Präfix erinnert Sie daran, wie das Schnellset erstellt wurde. Wie beliebige andere Standardsets können Schnellsets für ein einzelnes Gerät *individualisiert*, mit Auto-Lernen verwendet, für andere Benutzer freigegeben und über den VSA auf ähnliche Geräte angewendet werden.

1. Ermitteln Sie SNMP-Geräte über Monitor > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor > **SNMP zuweisen** *(siehe 340)* den ermittelten Geräten zu.
3. Klicken Sie auf der Seite **SNMP zuweisen** auf den Hyperlink unterhalb des Namens des Geräts (**SNMP-Info** *(siehe 345)*-Link), um einen Dialog anzuzeigen.

- Klicken Sie auf **Gefundene MIB-Objekte** und wählen Sie mindestens ein MIB-Objekt aus, das auf dem gerade ausgewählten SNMP-Gerät gefunden wurde.
- Klicken Sie auf **Schnellset-Elemente** und bearbeiten Sie bei Bedarf die Alarmschwellenwerte für ausgewählte MIB-Objekte.
- Geben Sie in der Kopfzeile des Dialogfelds den Namen nach dem Präfix **(QS)** ein.
- Klicken Sie auf die Schaltfläche **Anwenden**, um das Schnellset auf das Gerät anzuwenden.

4. Zeigen Sie vom Schnellset zurückgegebene SNMP-Monitordaten über Monitor > **SNMP-Protokoll** *(siehe 349)* genau so an, wie Sie es bei einem anderen Standard-SNMP-Set tun würden.
5. Die Pflege des neuen Schnellsets kann wahlweise mit Monitor > **SNMP-Sets** *(siehe 629)* erfolgen.

So erstellen Sie einen SNMP-Alarm:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
2. Legen Sie weitere E-Mail-Parameter fest.
3. Wählen Sie das SNMP-Set aus, das hinzugefügt oder ersetzt werden soll.
4. Markieren Sie die SNMP-Geräte, auf die der Alarm angewendet werden soll.
5. Klicken Sie auf die Schaltfläche **Apply**.

So brechen Sie einen SNMP-Alarm ab:

1. Aktivieren Sie das Kontrollkästchen für das SNMP-Gerät.
2. Klicken Sie auf die Schaltfläche **Löschen**.

   Die neben dem SNMP-Gerät aufgeführten Meldungsinformationen werden gelöscht.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitor-Meldungs-E-Mails können gesendet und formatiert werden:

- Monitoring des Schwellenwertalarms
- Monitoring des Trendschwellenwertalarms
- Benachrichtigung über Monitoring des Endalarmstatus

> **Hinweis:** Durch Ändern des E-Mail-Alarm-Formats wird das Format für *alle* Monitor-Set- und SNMP-Set-E-Mails geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung
<ad>	#ad#	Alarmdauer
<ao>	#ao#	Alarm-Betreiber
<um>	#at#	Alarmzeit
<av>	#av#	Alarmschwellenwert
<cg>	#cg#	Ereigniskategorie
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank

		ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.
<dv>	#dv#	SNMP-Gerätename
<gr>	#gr#	Gruppen-ID
<id>	#id#	Rechner-ID
<ln>	#ln#	Monitoring-Protokoll-Objektname
<lo>	#lo#	Monitoring-Protokoll-Objekttyp: Zähler, Prozess, Objekt
<lv>	#lv#	Monitoring-Protokollwert
<mn>	#mn#	Monitor-Set-Name
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.

- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden.**
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

(Filter anwenden)

Geben Sie Text in das Filter-Bearbeitungsfeld ein und klicken Sie auf das Trichtersymbol, um die Filterung auf die in **SNMP-Set auswählen** angezeigte Dropdown-Liste anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in dem Satznamen gefunden wird.

SNMP-Set auswählen

Wählen Sie SNMP-Sets aus der Liste **SNMP-Set auswählen** aus und klicken Sie auf **Anwenden**, um das SNMP-Set allen ausgewählten Rechner-IDs zuzuweisen. Sie können einer Rechner-ID mehr als ein SNMP-Set zuweisen. Das Hinzufügen oder Bearbeiten von SNMP-Sets erfolgt über Monitor > **SNMP-Sets** *(siehe 276)*.

> **Hinweis:** Beispiel-SNMP-Sets werden nicht in der Dropdown-Liste **SNMP zuweisen** *(siehe 340)* > **SNMP-Set auswählen** angezeigt. Erstellen Sie eine Kopie des Beispiel-SNMP-Sets, indem Sie das Beispielset in **SNMP-Sets** *(siehe 276)* auswählen und auf die Schaltfläche **Speichern unter** klicken. Ihre Kopie des Beispiel-SNMP-Sets wird in der Dropdown-Liste angezeigt. In einem **SaaS** *(siehe 631)*-basierten VSA sind die Schaltflächen **Speichern** und **Speichern unter** verfügbar. Sie können Änderungen am Beispielsatz vornehmen und diesen sofort verwenden, da er nicht aktualisiert wird.

Monitor-Set hinzufügen

Fügt das ausgewählte SNMP-Set den ausgewählten SNMP-Geräten zu.

Monitor-Set(s) ersetzen

Fügt das ausgewählten SNMP-Set den ausgewählten SNMP-Geräten zu und entfernt alle anderen SNMP-Sets, die dem ausgewählten SNMP-Gerät gegenwärtig zugewiesen sind.

SNMP-Liste bearbeiten

Fügen Sie manuell ein neues SNMP-Gerät hinzu oder bearbeiten Sie die Informationen vorhandener SNMP-Geräte. Geben Sie die IP- und MAC-Adresse sowie den Namen und eine Beschreibung des SNMP-Geräts ein. Sie können auch die Werte `sysDescr`, `sysLocation` und `sysContact` eingeben, die in der Regel vom Polling zurückgegeben werden.

Anwenden

Wendet das ausgewählte SNMP-Set auf die ausgewählten SNMP-Geräte an.

Löschen

Löscht die Zuweisung eines ausgewählten SNMP-Sets auf ausgewählten SNMP-Geräten.

Alle löschen

Löscht alle SNMP-Sets, die ausgewählten SNMP-Geräten zugewiesen sind.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Name/Typ

Der vom ARP-Protokoll zurückgegebene Name beim Durchführen eines **LAN-Watch**

(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)

Gerät-IP

Die IP-Adresse des SNMP-Geräts.

MAC-Adresse

Die MAC-Adresse des SNMP-Geräts

SNMP-INFO

Der vom SNMP-Protokoll zurückgegebene Name beim Durchführen eines LAN-Watch. Klicken Sie auf den Link **SNMP-Info** *(siehe 345)*, um die SNMP-Objekte für dieses SNMP-Gerät anzuzeigen.

SNMP-Sets

Zeigt die Liste der SNMP-Sets an, die einem SNMP-Gerät zugewiesen sind.

– **Bearbeiten** – Diese Option wird immer neben einem SNMP-Set angezeigt. Klicken Sie auf dieses Symbol, um Kopfzeilenparameter einzustellen, die mit denjenigen des ausgewählten SNMP-Geräts übereinstimmen.

– **Auto-Lernen-Werte überschreiben** – Diese Option wird angezeigt, wenn Auto-Lernen auf dieses standardmäßige SNMP-Set angewendet wurde. Klicken Sie auf dieses Symbol, um die tatsächlichen Werte anzuzeigen oder zu ändern, die mit **Auto-Lernen** *(siehe 332)* für dieses SNMP-Set auf diesem SNMP-Gerät berechnet wurden.

– **Individualisiertes SNMP-Set** – Diese Option wird angezeigt, wenn Auto-Lernen *nicht* auf dieses standardmäßige SNMP-Set angewendet wurde. Klicken Sie auf dieses Symbol, um ein **standardmäßiges SNMP-Set** *(siehe 276)* zu erstellen bzw. Änderungen an einer Kopie davon vorzunehmen, das spezifisch (individualisiert) für dieses SNMP-Gerät ist. *Bei einem individualisierten SNMP-Set wird dem Namen des SNMP-Sets ein (IND) Präfix vorangestellt.*

ATSE

Der ATSE-Antwortcode, der Rechner-IDs oder **SNMP-Geräten** *(siehe 629)* zugewiesen wird:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

SNMP-Schnellsets

Monitor > SNMP-Monitoring > SNMP zuweisen > SNMP-Info-Link

Auf der Seite **SNMP-Info** wird eine Liste der MIB-Objekte angezeigt, die von dem jeweils ausgewählten SNMP-Gerät bereitgestellt werden. Diese MIB-Objekte werden durch Ausführen eines beschränkten SNMP-Durchlaufs auf allen ermittelten SNMP-Geräten ermittelt, wann immer ein **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* stattfindet. Sie können die Liste der ermittelten MIB-Objekte verwenden, um sofort ein gerätespezifisches SNMP-Set mit der Bezeichnung **Schnellset** zu erstellen und auf das Gerät anzuwenden. Schnellsets entsprechen nach der Erstellung den Standardsets. Sie werden in Ihrem privaten Ordner in Monitor > **SNMP-Sets** und in der Dropdown-Liste in Monitor > **SNMP zuweisen** angezeigt. Ein `(QS)`-Präfix erinnert Sie daran, wie das Schnellset erstellt wurde. Wie beliebige andere Standardsets können Schnellsets für ein einzelnes Gerät *individualisiert*, mit Auto-Lernen verwendet, für andere Benutzer freigegeben und über den VSA auf ähnliche Geräte angewendet werden.

1. Ermitteln Sie SNMP-Geräte über Monitor > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor > **SNMP zuweisen** *(siehe 340)* den ermittelten Geräten zu.
3. Klicken Sie auf der Seite **SNMP zuweisen** auf den Hyperlink unterhalb des Namens des Geräts (**SNMP-Info** *(siehe 345)*-Link), um einen Dialog anzuzeigen.
   - Klicken Sie auf **Gefundene MIB-Objekte** und wählen Sie mindestens ein MIB-Objekt aus, das auf dem gerade ausgewählten SNMP-Gerät gefunden wurde.
   - Klicken Sie auf **Schnellset-Elemente** und bearbeiten Sie bei Bedarf die Alarmschwellenwerte für ausgewählte MIB-Objekte.
   - Geben Sie in der Kopfzeile des Dialogfelds den Namen nach dem Präfix **(QS)** ein.
   - Klicken Sie auf die Schaltfläche **Anwenden**, um das Schnellset auf das Gerät anzuwenden.
4. Zeigen Sie vom Schnellset zurückgegebene SNMP-Monitordaten über Monitor > **SNMP-Protokoll** *(siehe 349)* genau so an, wie Sie es bei einem anderen Standard-SNMP-Set tun würden.
5. Die Pflege des neuen Schnellsets kann wahlweise mit Monitor > **SNMP-Sets** *(siehe 629)* erfolgen.

Über die folgenden Registerkarten auf der Seite **SNMP-Info-Link** können Sie ein SNMP-Schnellset konfigurieren.

Registerkarte „Ermittelte MIB-Objekte“

Auf der Registerkarte **Ermittelte MIB-Objekte** werden alle beim letzten SNMP-Durchlauf ermittelten Objektsätze angezeigt, die für das angewählte SNMP-Gerät gelten. Sie können über diese Registerkarte Objekte und Instanzen zu einem SNMP-Schnellset für dieses Gerät hinzufügen.

- **Instanz hinzufügen** – Klicken Sie auf diese Option, um diese Instanz dieses Objekts zu einem SNMP-Schnellset hinzuzufügen, das auf der Registerkarte **SNMP-Set** des gleichen Fensters angezeigt wird.
- **Alle Instanzen hinzufügen** – Klicken Sie auf diese Option, um alle Instanzen dieses Objekts zu einem SNMP-Schnellset hinzuzufügen, das auf der Registerkarte **SNMP-Set** des gleichen Fensters angezeigt wird.
- **SNMP-Objekt** – Der Name des SNMP-Objekts. Wenn kein Name für das Objekt angegeben wird, wird die numerische OID-Bezeichnung angezeigt.
- **Instanz** – Die Instanz des Objekts. Viele Objekte haben mehrere Instanzen, von denen jedes einen anderen Wert haben kann. Als verschiedene Instanzen zählen beispielsweise die Ports eines Routers oder die Ablagefächer eines Druckers. Das Feld ist leer, wenn die letzte Ziffer der OID Null ist, was darauf hinweist, dass es nur ein Mitglied dieses Objekts gibt. Wenn eine Instanz nicht leer oder eine beliebige Zahl ungleich Null ist, so existieren mehrere Instanzen dieses Objekts für das Gerät. Sie können das Monitoring mehrerer Instanzen eines Objekts festlegen, indem Sie einen Zahlenbereich wie beispielsweise `1-5,6` oder `1,3,7` angeben. Sie können auch `All` eingeben.
- **Aktueller SNMP-Wert** – Der beim letzten SNMP-Durchlauf von der Objekt/Instanz-Kombination zurückgegebene Wert

Schnellset-Elemente – Registerkarte

Auf der Registerkarte **Schnellset-Elemente** konfigurieren Sie die ausgewählten Objekte und Instanzen, die in das SNMP-Schnellset eingeschlossen werden sollen. Klicken Sie auf das Bearbeitungssymbol, um die SNMP-Kontrollattribute für die ausgewählten Objekte zu definieren. Sie können auch mithilfe der Schaltfläche **Hinzufügen** ein neues Objekt hinzufügen und die gleichen Attribute festlegen.

- **SNMP-Objekt** – Der SNMP-Objektname oder die OID-Nummer.
- **SNMP-Instanz** – Die letzte Zahl einer Objekt-ID kann auch als eine Wertetabelle statt eines einzelnen Werts ausgedrückt werden. Falls die Instanz ein einzelner Wert ist, geben Sie `0` ein. Wenn die Instanz eine Wertetabelle ist, geben Sie einen Zahlenbereich ein, wie beispielsweise `1-5,6` oder `1,3,7`. Sie können auch `All` eingeben.

- **Alarm-Operator** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen Changed, Equal oder NotEqual. Für numerische Rückgabewerte lauten die Optionen Equal, NotEqual, Over oder Under..
- **Alarmschwellenwert** – Legt einen festen Wert fest, mit dem der Rückgabewert verglichen wird, und verwendet den ausgewählten **Alarm-Operator**, um festzulegen, wann ein Alarm ausgelöst wird.
- **Wert zurückgegeben als** – Wenn das MIB-Objekt einen numerischen Wert zurückgibt, können Sie angeben, ob dieser Wert als eine **Summe** oder als eine **Rate pro Sekunde** zurückgegeben werden soll.
- **Aktueller SNMP-Wert** – Der beim letzten SNMP-Durchlauf von der Objekt/Instanz-Kombination zurückgegebene Wert
- Registerkarte SNMP-Sets

Registerkarte SNMP-Symbole

- Passen Sie die Alarmsymbole für dieses *spezifische SNMP-Schnellset* an. Allgemeine Erläuterungen zu Verwendung dieser Seite finden Sie unter **SNMP-Symbole** *(siehe 283)*.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Übernehmen

Speichert die an dieser Seite vorgenommenen Änderungen.

Abbrechen

Mit dieser Option werden alle auf dieser Seite vorgenommenen Änderungen ignoriert und Sie kehren zur Liste der SNMP-Sets zurück.

Löschen

Löscht alle SNMP-Objekte auf allen Registerkarten. Einige Minuten später wird wieder die Standardliste der Objekte in **Ermittelte Objektsätze** eingetragen.

Auto-Lernen – SNMP-Sets

Monitor > SNMP-Monitoring > SNMP zuweisen > Auto-Lernen

Über das Fenster **Auto-Lernen-Alarmschwellenwerte** werden die Auto-Lernen-Alarmschwellenwerte für SNMP-Sets gepflegt.

Sie können **Auto-Lernen**-Alarmschwellenwerte für jedes beliebige SNMP-Set bzw. -Schnellset aktivieren, das Sie ausgewählten SNMP-Geräten zuweisen. Damit werden Alarmschwellenwerte basierend auf tatsächlichen Leistungsdaten auf die einzelnen SNMP-Geräte abgestimmt.

Jedes zugewiesene SNMP-Gerät generiert Leistungsdaten für die angegebene Zeitspanne. Während dieser Zeitspanne werden keine Alarme ausgelöst. Am Ende der **Auto-Lernen**-Sitzung wird der Alarmschwellenwert für jedes zugewiesene SNMP-Gerät basierend auf der tatsächlichen Leistung des SNMP-Geräts automatisch abgestimmt. Sie können die Alarmschwellenwerte, die durch **Auto-Lernen** berechnet wurden, manuell anpassen oder eine weitere **Auto-Lernen**-Sitzung ausführen. **Auto-Lernen** kann nicht mit individualisierten SNMP-Sets verwendet werden

So wenden Sie **Auto-Lernen**-Einstellungen auf ausgewählte SNMP-Geräte an:

1. Wählen Sie ein *Standard*-SNMP-Set aus der <Select SNMP Set>-Dropdown-Liste aus. Sie können auch auf das Bearbeitungssymbol eines SNMP-Sets klicken, der bereits einem Gerät zugeordnet ist, um den Identifikator in die <Select SNMP Set>-Dropdown-Liste zu übertragen.

2. Klicken Sie auf **Auto-Lernen**, um das Popup-Fenster **Auto-Lernen** *(siehe 332)* einzublenden. Definieren Sie mithilfe eines Assistenten die Parameter, die zum Berechnen der Alarmschwellenwerte verwendet werden.
3. Weisen Sie dieses Standard-SNMP-Set, das durch Ihre **Auto-Lernen**-Parameter abgeändert wurde, ausgewählten SNMP-Geräten zu, falls dies noch nicht geschehen ist.

Sobald **Auto-Lernen** auf eine Rechner-ID angewendet und für die vorgegebene Zeitspanne ausgeführt wurde, können Sie für ein bestimmtes SNMP-Gerät auf das Auto-Lernen-überschreiben-Symbol klicken und die berechneten Alarmschwellenwerte manuell anpassen. Sie können auch **Auto-Lernen** in einer neuen Sitzung unter Verwendung der tatsächlichen Leistungsdaten erneut ausführen, um die Alarmschwellenwerte neu zu berechnen.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Bearbeiten

Klicken Sie auf das Bearbeitungssymbol, um einen Assistenten aufzurufen, der Sie durch die drei Schritte zum Bearbeiten von Auto-Lernen-Alarmschwellenwerten führt.

1. Aktivieren Sie Auto-Lernen für dieses SNMP-Objekt, indem Sie `Yes - Include` auswählen. Wenn `No - Do not include` ausgewählt ist, sind keine weiteren Auswahlen in diesem Assistenten zutreffend.
   - **Zeitspanne** – Geben Sie an, wie lange Leistungsdaten erfasst und zur automatischen Berechnung der Alarmschwellenwerte verwendet werden sollen. Während dieser Zeitspanne werden keine Alarme gemeldet.
2. Zeigt das **SNMP-Objekt** des geänderten Alarmschwellenwerts an. Diese Option kann nicht geändert werden.
   - **Schnittstelle**
3. Geben Sie Parameter für die Wertberechnung ein.
   - **Berechnung** – Geben Sie einen Parameter für die Wertberechnung ein. Mögliche Optionen sind `MIN`, `MAX` oder `AVG`. Bei Auswahl von `MAX` wird beispielsweise der maximale Wert berechnet, der für ein SNMP-Objekt während der oben angegebenen **Zeitspanne** erfasst wurde.
   - **% Anstieg** – Fügen Sie diesen Anstieg zu dem oben berechneten **Berechnung**swert hinzu, wobei der **Berechnung**swert 100% darstellt. Der resultierende Wert stellt den Alarmschwellenwert dar.
   - **Minimum** – Legen Sie einen Mindestwert für den Alarmschwellenwert fest. Dieser Wert wird automatisch als *zwei Standardabweichungen unter* dem berechneten **Berechnung**swert berechnet, doch dieser Wert kann manuell überschrieben werden.
   - **Maximum** – Legen Sie einen Maximalwert für den Alarmschwellenwert fest. Dieser Wert wird automatisch als *zwei Standardabweichungen über* dem berechneten **Berechnung**swert berechnet, doch dieser Wert kann manuell überschrieben werden.

Weiter

Damit gelangt der Benutzer zur nächsten Seite im Assistenten.

Zurück

Damit gelangt der Benutzer zur vorherigen Seite im Assistenten.

Abbrechen

Mit dieser Option werden alle auf dieser Seite vorgenommenen Änderungen ignoriert und Sie kehren zur Liste der **Zählerobjekte** zurück.

Speichern

Speichert die an den Seiten des Assistenten vorgenommenen Änderungen.

SNMP-Protokoll

Monitor > SNMP-Monitoring > SNMP-Protokoll

Auf der Seite **SNMP-Protokoll** werden SNMP-Protokolldaten der **MIB-Objekte** *(siehe 629)* in einem **SNMP-Set** *(siehe 276)* als Diagramm oder in tabellarischer Form angezeigt.

1. Klicken Sie auf einen Rechner-ID-Link, um alle mit einer Rechner-ID verknüpften SNMP-Geräte anzuzeigen.
2. Klicken Sie auf eine IP-Adresse oder den Namen eines SNMP-Geräts, um alle SNMP-Sets und MIB-Objekte anzuzeigen, die diesem SNMP-Gerät zugewiesen sind.
3. Klicken Sie auf das Erweiterungssymbol ⊞, um die Erfassungs- und Schwellenwerteinstellungen für ein MIB-Objekt anzuzeigen.
4. Klicken Sie auf die Pfeiltaste nach unten ⊡, um die Protokolldaten des MIB-Objekts als Diagramm oder Tabelle anzuzeigen.
5. Aktivieren Sie das Optionsfeld **Balkendiagramm** oder **Tabelle**, um die Protokolldaten im gewünschten Format anzuzeigen.

SNMP-Monitor-Objekte können mehrere Instanzen enthalten und gemeinsam in einem Diagramm oder einer Tabelle angezeigt werden. Ein Netzwerkschalter kann beispielsweise 12 Ports umfassen. Jeder ist eine Instanz und kann Protokolldaten enthalten. Alle 12 Instanzen können zu einem Diagramm oder einer Tabelle zusammengefasst werden. SNMP-Balkendiagramme liegen im 3D-Format vor, was die Ansicht mehrerer Instanzen ermöglicht.

Rechner-ID.Gruppen-ID/SNMP-Geräte

Alle Rechner, denen SNMP-Monitoring zugewiesen ist, und die dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* entsprechen, werden angezeigt. Durch Klicken auf diesen Rechner-ID-Link werden alle SNMP-Geräte angezeigt, die mit der Rechner-ID verknüpft sind. Klicken Sie auf den Link für das SNMP-Gerät, um alle mit diesem SNMP-Gerät verknüpften MIB-Objekte anzuzeigen.

Ansicht

Klicken Sie auf den Link **Ansicht**, um die Protokolldaten für ein MIB-Objekt in einem Diagramm oder einer Tabelle anzuzeigen.

Entfernen

Klicken Sie auf **Entfernen**, um die Protokolldaten aus einem Diagramm oder einer Tabelle zu entfernen.

Alle anzeigen

Falls das SNMP-Monitor-Objekt mehrere Instanzen umfasst, werden durch Klicken auf **Alle anzeigen** alle Daten für alle Instanzen angezeigt.

Alle entfernen

Falls das SNMP-Monitor-Objekt mehrere Instanzen umfasst, werden durch Klicken auf **Alle entfernen** alle Daten für alle Instanzen entfernt.

Name des Monitor-Sets

Der Name des SNMP-Sets, zu dem das MIB-Objekt gehört

Objektnamen abrufen

Der Name des MIB-Objekts, das für die Überwachung des SNMP-Geräts verwendet wird

Beschreibung

Die Beschreibung des MIB-Objekts in dem SNMP-Set

Balkendiagramm/Tabelle

Aktivieren Sie das Optionsfeld **Balkendiagramm** oder **Tabelle**, um die Daten im gewünschten Format anzuzeigen.

- In einem Balkendiagramm werden die letzten 2000 Datenpunkte für die Abfrageintervallfrequenz dargestellt. Der Hintergrund des Diagramms ist rot für Alarmschwellenwert, gelb für Warnungsschwellenwert und grün, wenn kein Alarm.
- In den Tabellenprotokolldaten werden die aktuellen Werte zuerst aufgeführt. Außerdem werden Alarm- und Warnungssymbole für Protokolldaten angezeigt, die in diese Schwellenwerte fallen. Weitere Informationen finden Sie unter **SNMP-Set definieren** *(siehe 278)*.

Letzte anzeigen

In einem Balkendiagramm werden die Protokolldaten für die letzte Anzahl an Intervallen dargestellt. Wenn Sie beispielsweise **Letzte 500 Minuten** auswählen, stellt jeder Balken in dem Diagramm 1 Minute dar.

Ansicht speichern

Sie können für jedes MIB-Objekt benutzerdefinierte Ansichten speichern. Wenn dieses MIB-Objekt das nächste Mal ausgewählt wird, werden die gespeicherten Informationen geladen.

Protokollzeilen pro Seite

Diese Felder werden nur im **Tabellen**format angezeigt. Wählen Sie die Anzahl der Zeilen aus, die pro Seite angezeigt werden sollen.

Wert über/unter anzeigen

Diese Felder werden nur im **Tabellen**format angezeigt. Filtern Sie die Tabellenzeilen, indem Sie Protokolldaten, die über oder unter dem angegebenen Wert liegen, herausfiltern.

Aktualisieren

Klicken Sie auf „Aktualisierungen“, um nur die aktuellen Protokolldaten anzuzeigen.

Falls der Monitor keine Protokollwerte anzeigt, überprüfen Sie Folgendes:

1. Falls keine Werte zurückgegeben wurden, prüfen Sie den Erfassungsschwellenwert für MIB-Objekte in SNMP-Sets. Falls keine Werte auf dem überwachten Gerät den Erfassungsschwellenwert erfüllen, werden diese nicht in das SNMP-Protokoll aufgenommen.
2. Das Abfrageintervall für den Protokollwert ergibt sich aus der Gesamtanzahl der `SNMPGet`-Befehle, mit denen Informationen von SNMP-Geräten ermittelt und dem Agent der Rechner-ID zur Verfügung gestellt werden. Je mehr `SNMPGet`-Befehle Sie verwenden, desto größer ist das Abfrageintervall. Prüfen Sie alle mit einer Rechner-ID verknüpften SNMP-Geräte. Wenn einige `SNMPGet`-Befehle Werte zurückgeben, andere hingegen nicht, sind die `SNMPGet`-Befehle für die fehlgeschlagenen Abfragen nicht kompatibel.

Wenn ein Monitor nicht reagiert, erscheint im Protokoll die Meldung `Monitor Not Responding`. Der `SNMPGet`-Befehl ist mit dem Gerät nicht kompatibel.

SNMP-Werte einrichten

Monitor > SNMP-Monitoring > SNMP-Werte einstellen

Über die Seite **SNMP-Werte einstellen** können Sie Werte an SNMP-Netzwerkgeräte schreiben. Für die SNMP-Objekte muss `Read Write` aktiviert sein. Außerdem ist die Eingabe des Write Community-Passworts für das SNMP-Gerät erforderlich.

Eine SNMP-Community ist eine Gruppierung von Geräten und Managementstationen, auf denen SNMP ausgeführt wird. SNMP-Informationen werden an alle Mitglieder der gleichen Community in einem Netzwerk gesendet. Die Standard-SNMP-Communities sind:

- Write = privat
- Read = öffentlich

Hinweis: Diese Seite wird nur für Rechner angezeigt, die zuvor durch ein **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* identifiziert wurden.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner-ID.Gruppen-ID

Listet die **Rechner-ID.Gruppen-IDs** *(siehe 626)* auf, die gegenwärtig dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* entsprechen und denen ein **SNMP Community** *(siehe 629)*-Name zugewiesen ist. Klicken Sie auf eine Rechner-ID, um alle mit dieser Rechner-ID verknüpften SNMP-Geräte anzuzeigen.

SNMP-Gerät

Wählen Sie das gewünschte SNMP-Gerät aus. Dadurch wird eine Historie der SNMPSet-Werte angezeigt, die vom Agent der Rechner-ID an ein SNMP-Gerät geschrieben wurden.

SNMPSet-Befehl erstellen

Klicken Sie auf **SNMPSet-Befehl erstellen**, um einen neuen Wert an dieses SNMP-Gerät zu schreiben. Die folgenden Felder werden angezeigt:

- **Beschreibung** – Geben Sie eine leicht einzuprägende Beschreibung dieses Ereignisses ein. Dadurch wird die Historie der SNMPSet-Werte für dieses SNMP-Gerät angezeigt.
- **MIB-Objekt** – Wählen Sie das **MIB-Objekt** *(siehe 629)* aus. Klicken Sie auf **Objekt hinzufügen** *(siehe 281)*, um auf der Seite **Monitorlisten** *(siehe 264)* ein MIB-Objekt hinzuzufügen, das gegenwärtig nicht existiert.
- **SNMP-Version** – Wählen Sie eine SNMP-Version aus. Version 1 wird von allen Geräten unterstützt (Standard). Version 2c definiert mehr Attribute, die zurückgegeben werden können, und verschlüsselt die Pakete an den und von dem SNMP-Agent. Wählen Sie Version 2c nur dann aus, wenn Sie sicher sind, dass das Gerät die Version 2c unterstützt.
- **writeCommunity** – Das Write Community-Passwort für das SNMP-Gerät. Das Standardpasswort der Write Community ist `private`.
- **timeOutValue** – Geben Sie die Anzahl der Sekunden an, die auf eine Antwort des SNMP-Geräts gewartet werden soll, bevor eine Zeitüberschreitung des Write-Befehls eintritt.
- **setValue** – Geben Sie den Wert ein, auf den das ausgewählte MIB-Objekt auf dem SNMP-Gerät eingestellt werden soll.
- **attempts** – Geben Sie an, wie oft versucht werden soll, in das MIB-Objekt zu schreiben, wenn der Write-Befehl beim ersten Mal nicht akzeptiert wird.

SNMPSet ausführen

Bereitet ein Verfahren vor, das einen SNMPSet-Befehl für das ausgewählte SNMP-Gerät ausführt.

Abbrechen

Ignoriert alle eingegebenen Daten und zeigt erneut den Link **SNMP-Befehl erstellen** und die Historie an.

SNMP-Typ konfigurieren

Monitor > SNMP-Monitoring > SNMP-Typ konfigurieren

Über die Seite **SNMP-Typ konfigurieren** werden den SNMP-Geräten *manuell* bestimmte Typen zugewiesen. SNMP-Geräten, denen einer dieser Typen zugewiesen wird, werden über SNMP-Sets dieses Typs überwacht. Sie können für einzelne SNMP-Geräte auch benutzerdefinierte Namen und Beschreibungen eingeben bzw. ein Gerät aus der Datenbank entfernen.

Die meisten SNMP-Geräte werden mithilfe des MIB-Objekts `system.sysServices.0` als ein bestimmter SNMP-Gerätetyp klassifiziert. Beispielsweise identifizieren sich einige Router selbst generisch als Router, indem sie den Wert `77` für das MIB-Objekt `system.sysServices.0` zurückgeben. Sie können den vom MIB-Objekt `system.sysServices.0` zurückgegebenen Wert verwenden, um SNMP-Sets automatisch zu Geräten zuzuweisen, sobald sie von einem LAN-Watch erkannt wurden.

> **Hinweis:** Die gesamte OID für `system.sysServices.0` ist `.1.3.6.1.2.1.1.7.0` oder `.iso.org.dod.internet.mgmt.mib-2.system.sysServices`.

Weisen Sie folgendermaßen **SNMP-Sets** *(siehe 629)* bestimmten **Geräten** *(siehe 629)* *automatisch nach Typ* zu:

1. Fügen Sie SNMP-*Typen* über die Registerkarte **SNMP-Gerät** in Monitor > **Monitorlisten** *(siehe 264)* hinzu bzw. bearbeiten Sie sie.
2. Fügen Sie den vom MIB-Objekt `system.sysServices.0` zurückgegebenen *und mit dem jeweiligen SNMP-Typ verknüpften* Wert hinzu bzw. bearbeiten Sie ihn mithilfe der Registerkarte **SNMP-Dienste** in Monitor > **Monitorlisten**.
3. Verknüpfen Sie einen SNMP-*Typ* über die Dropdown-Liste **Automatische Bereitstellung auf** in Monitor > SNMP-Sets > **SNMP-Set definieren** *(siehe 278)* mit einem SNMP-*Set*.
4. Führen Sie einen **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* durch. Während des LAN-Watch werden SNMP-Sets automatisch zugewiesen, um von SNMP-Sets überwacht zu werden, wenn das SNMP-Gerät einen Wert für das MIB-Objekt `system.sysServices.0` zurückgibt, der dem SNMP-Typ entspricht, der mit diesen SNMP-Sets verknüpft ist.

Weisen Sie folgendermaßen **SNMP-Sets** *(siehe 629)* bestimmten **Geräten** *(siehe 629)* *manuell* zu:

1. Mit Monitor > **SNMP-Typ konfigurieren** *(siehe 352)* können Sie einen SNMP-Typ einem SNMP-Gerät zuweisen. In diesem Fall beginnt das System automatisch mit dem Monitoring dieses SNMP-Geräts anhand dieses SNMP-Sets.

Zuweisen

Wendet den ausgewählten SNMP-Typ auf die ausgewählten SNMP-Geräte an.

Löschen

Entfernt die ausgewählten SNMP-Geräte aus der Datenbank. Falls das Gerät beim nächsten Durchführen eines LAN-Watch immer noch vorliegt, wird es wieder zur Datenbank hinzugefügt. Dies ist nützlich bei Änderungen der IP- oder MAC-Adresse eines Geräts.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Name

Liste der SNMP-Geräte, die durch ein **LAN Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* für eine bestimmte Rechner-ID generiert wurde.

Typ

Der dem SNMP-Gerät zugewiesene SNMP-Typ

Benutzerdefinierter Name

Der benutzerdefinierte Name und die benutzerdefinierte Beschreibung des SNMP-Geräts. Falls Sie einem Gerät einen benutzerdefinierten Namen geben, wird dieser anstelle des SNMP-Namens und der IP-Adresse in Alarmen und im SNMP-Protokoll angezeigt. Um den benutzerdefinierten Namen und die Beschreibung zu ändern, klicken Sie auf das Bearbeitungssymbol neben dem benutzerdefinierten Namen.

Gerät-IP

Die IP-Adresse des SNMP-Geräts.

MAC-Adresse

Die MAC-Adresse des SNMP-Geräts

SNMP-Name

Der Name des SNMP-Geräts.

Parser-Übersicht

Monitor > Protokoll-Monitoring > Analyseübersicht

Auf der Seite **Analyseübersicht** werden die Meldungen für alle Analysesätze angezeigt, die allen Rechner-IDs innerhalb des Umfangs des Benutzers zugewiesen sind. Außerdem können diese wahlweise definiert werden. Darüber hinaus können auf der Seite **Analyseübersicht** Analysesatz-Zuweisungen auf mehrere Rechner-IDs kopiert werden.

> **Hinweis:** Durch Kopieren eines Analysesatzes auf eine Rechner-ID auf dieser Seite wird die Protokollanalyse auf diesen Rechner-IDs *aktiviert*. Eine Analyse findet statt, wann immer die analysierte Protokolldatei aktualisiert wird.
>
> **Hinweis:** Unter dem ersten Thema der Online-Hilfe können Sie die PDF-Datei **Schrittweise Konfiguration von Protokollanalysen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_logparsers70.pdf#zoom=70&navpanes=0)* herunterladen.

Protokoll-Monitoring, Setup

1. **Protokollanalyse** – Identifizieren Sie eine Protokolldatei, die anhand einer Protokolldatei-Analysedefinition analysiert werden soll. Eine Protokolldatei-Analysedefinition umfasst die Protokolldateiparameter, die zum Speichern der aus der Protokolldatei extrahierten Werte verwendet werden. Anschließend weisen Sie die Protokollanalyse einem oder mehreren Rechnern zu.

2. **Analysesätze zuweisen** – Definieren Sie einen Analysesatz, um Protokollkontrolldatensätze basierend auf den spezifischen in den Parametern gespeicherten Werten zu generieren. *Aktivieren* Sie die Analyse, indem Sie den Analysesatz einer oder mehreren Rechner-IDs zuweisen, denen Sie zuvor diese Protokollanalyse zugewiesen haben. Definieren Sie wahlweise Meldungen.
3. **Analyseübersicht** – Kopieren Sie auf schnelle Weise *aktive* Analysesatzzuweisungen von einem einzelnen Rechner auf andere Rechner-IDs. Definieren Sie wahlweise Meldungen.

Benachrichtigung

Der Agent erfasst Protokolleinträge und erstellt einen Eintrag im „Protokoll-Monitoring"-Protokoll, basierend auf den im Analysesatz definierten Kriterien, *egal, ob irgendwelche Benachrichtigungsmethoden aktiviert sind oder nicht.* Sie brauchen nicht jedes Mal benachrichtigt zu werden, wenn ein neuer Protokoll-Monitoring-Eintrag erstellt wird. Sie können einfach nach Bedarf **das „Protokoll-Monitoring"-Protokoll überprüfen** *(siehe 369)*.

So kopieren Sie Analysesatz-Zuweisungen:

1. Wählen Sie einen Quellrechner aus, von dem die Analysesatz-Zuweisungen kopiert werden sollen.
2. Wählen Sie die Rechner-IDs aus, auf die die Analysesatz-Zuweisungen kopiert werden sollen.
3. Klicken Sie auf **Kopieren**.

So erstellen Sie einen Analysesatz-Alarm:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
2. Legen Sie weitere E-Mail-Parameter fest.
3. Markieren Sie die Rechner-IDs, auf die der Alarm angewendet werden soll.
4. Klicken Sie auf die Schaltfläche **Apply**.

So brechen Sie einen Analysesatz-Alarm ab:

1. Aktivieren Sie das Kontrollkästchen für die Rechner-ID.
2. Klicken Sie auf die Schaltfläche **Löschen**.

   Die neben der Rechner-ID aufgeführten Meldungsinformationen werden gelöscht.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitoring-Meldungs-E-Mails können gesendet und formatiert werden:

- Warnungen zu Protokollkontrollanalysen.
- Warnungen zu mehreren Protokollkontrollanalysen.
- Warnung zu fehlender Protokollkontrollanalyse.

> **Hinweis:** Durch Ändern dieses E-Mail-Alarmformats wird das Format von **Analysesätze zuweisen** und **Analyseübersicht** geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind. Ein ● in einer nummerierten Spalte gibt an, dass eine Variable mit dem Meldungstyp, der dieser Nummer entspricht, verwendet werden kann.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung	1	2	3
<ad>	#ad#	duration		●	
<um>	#at#	Alarmzeit	●	●	●
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.	●	●	●
<ec>	#ec#	Ereigniszählung		●	
<ed>	#ed#	Ereignisbeschreibung	●	●	
<gr>	#gr#	Gruppen-ID	●	●	●
<id>	#id#	Rechner-ID	●	●	●
<lpm>	#lpm#	Protokolldateisatz-Kriterien	●	●	●
<lpn>	#lpn#	Name des Protokollanalysesatzes	●	●	●
<lsn>	#lsn#	Name des Protokolldateisatzes	●	●	●
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.

- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Kopie

Klicken Sie auf **Kopieren**, um die Analysesätze der ausgewählten Rechner-ID unter Verwendung des Links **diese Rechner-ID** auf andere im Seitenbereich ausgewählte Rechner-IDs zu kopieren.

Anwenden

Wendet die Alarm-Einstellungen auf die ausgewählten Rechner-IDs an.

Alle löschen

Löscht alle Alarm-Einstellungen von ausgewählten Rechner-IDs.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Löschen

Klicken Sie auf das Löschen-Symbol neben einem Analysesatz, um dessen Zuweisung zu einer Rechner-ID zu löschen.

Protokollsatznamen

Listet die Namen der dieser Rechner-ID zugewiesenen Analysesätze auf.

ATSE

Der den Rechner-IDs zugewiesene ATSE-Antwortcode:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Verfahren ausführen

- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Intervall

Gibt das Intervall an, das abgewartet werden soll, um festzustellen, ob ein Ereignis eintritt oder nicht.

Dauer

Gilt nur, wenn die Option **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden> eintritt** aktiviert ist. Bezieht sich auf **<N> <Perioden>**.

Wiederherstellen

Gilt nur, wenn die Option **Zusätzliche Alarme übergehen für <N> <Perioden> aktiviert ist.**

Log-Parser

Monitor > Protokoll-Monitoring > Protokollanalyse

Über die Seite **Protokollanalyse** definieren Sie Protokollanalysen und weisen diese ausgewählten Rechner-IDs zu.

> **Hinweis:** Unter dem ersten Thema der Online-Hilfe können Sie die PDF-Datei **Schrittweise Konfiguration von Protokollanalysen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_logparsers70.pdf#zoom=70&navpanes=0)* herunterladen.
>
> **Hinweis:** Die Protokollanalysen sind nur *aktiv* , wenn sie anschließend mit **Analysesätze zuweisen** *(siehe 363)* einem Protokollanalysesatz zugewiesen werden.

Protokoll-Monitoring

Der VSA kann die aus zahlreichen **Standardprotokolldateien** *(siehe 625)* gesammelten Daten überwachen. **Protokoll-Monitoring** erweitert diese Fähigkeit noch weiter, indem Daten von der Ausgabe einer beliebigen textbasierten Protokolldatei extrahiert werden können. Beispiele hierfür sind Anwendungsprotokolldateien und **syslog** *(siehe 631)*-Dateien, die für Unix-, Linux- und Apple-Betriebssysteme und für Netzwerkgeräte wie etwa Cisco-Router erstellt wurden. Damit nicht alle in diesen Protokollen enthaltenen Daten in die Kaseya Server-Datenbank hochgeladen werden, verwendet die **Protokoll-Monitoring Analysedefinitionen und Analysesätze** *(siehe 613)* zum Analysieren jeder Protokolldatei und wählt nur diejenigen Daten aus, an denen Sie interessiert sind. Analysierte Nachrichten werden im Protokoll-Monitoring angezeigt, das Sie über die Registerkarte „Agent-Protokolle" der Seite **Live Connect** *(siehe 393)* > Agent-Daten oder **Rechnerübersicht** *(siehe 151)* oder durch Generieren eines Berichts über die Seite Agent > Protokolle > **Protokoll-Monitoring** *(siehe 221)* aufrufen können. Benutzer können wahlweise beim Generieren eines **Protokoll-Monitoring**-Datensatzes Meldungen auslösen, laut Definition mit **Analysesätze zuweisen** *(siehe 363)* oder **Analyseübersicht** *(siehe 353)*.

Protokoll-Monitoring, Setup

1. **Protokollanalyse** – Identifizieren Sie eine Protokolldatei, die anhand einer Protokolldatei-Analysedefinition analysiert werden soll. Eine Protokolldatei-Analysedefinition umfasst die Protokolldateiparameter, die zum Speichern der aus der Protokolldatei extrahierten Werte verwendet werden. Anschließend weisen Sie die Protokollanalyse einem oder mehreren Rechnern zu.
2. **Analysesätze zuweisen** – Definieren Sie einen Analysesatz, um Protokollkontrolldatensätze basierend auf den spezifischen in den Parametern gespeicherten Werten zu generieren. *Aktivieren* Sie die Analyse, indem Sie den Analysesatz einer oder mehreren Rechner-IDs

zuweisen, denen Sie zuvor diese Protokollanalyse zugewiesen haben. Definieren Sie wahlweise Meldungen.

3. **Analyseübersicht** – Kopieren Sie auf schnelle Weise *aktive* Analysesatzzuweisungen von einem einzelnen Rechner auf andere Rechner-IDs. Definieren Sie wahlweise Meldungen.

Der Protokolldateianalysezyklus

Die Analyse einer Protokolldatei wird bei jeder Änderung der Protokolldatei ausgelöst. In den meisten Fällen bedeutet dies das Anhängen von neuem Text an das Ende der Datei. Um zu vermeiden, dass bei jeder Aktualisierung der Datei die gesamte Protokolldatei von Anfang an gescannt wird, parst der Agent Protokolldateien wie folgt:

- Der Agent speichert nach jeder Aktualisierung ein "Lesezeichen" der letzten 512 Byte einer Protokolldatei.
- Wird die Protokolldatei erneut aktualisiert, vergleicht der Agent das Lesezeichen der alten Aktualisierung mit der *gleichen Byteposition* in der neuen Aktualisierung.
- Da Protokolldateien eventuell vor Ausführen der Protokollanalyse archiviert werden, kann die Analyse auch Archivdateien einschließen, sofern vorhanden.
- Durch Angabe vollständiger Pfadnamen mit Sternchen (*) und Fragezeichen (?) als Stellvertreterzeichen können Sie bestimmte Sätze von Protokoll- und Archivdateien festlegen. Wenn ein Satz von Dateien angegeben wurde, beginnt der Parser mit der letzten Datei in dem Satz.
- Wenn der Lesezeichentext in der alten und neuen Aktualisierung identisch ist, beginnt der Agent mit der Analyse des Texts *nach dem Lesezeichen*.
- Falls der Lesezeichentext in den beiden Versionen *nicht* identisch ist und kein Protokollarchivpfad angegeben wurde, analysiert der Agent die gesamte Protokolldatei von Anfang an. Falls ein Protokollarchivpfad angegeben wurde, sucht der Agent in den Archivdateien nach dem Lesezeichen. Wenn das Lesezeichen nicht auffindbar ist, markiert der Agent das Ende der Protokolldatei und beginnt beim nächsten Zyklus an diesem Punkt mit der Analyse.
- Sobald die Analyse abgeschlossen ist, wird ein neues Lesezeichen basierend auf den letzten 512 Byte der neu aktualisierten Protokolldatei definiert und der Prozess wiederholt sich.

> **Hinweis:** Die Analyse einer Protokolldatei selbst gilt nicht als Verfahrensereignis. Nur eine erneute Konfiguration oder Neukonfiguration unter Verwendung von **Protokollanalyse**, **Analysesätze zuweisen** oder **Analyseübersicht** generiert ein Verfahren, das auf den Registerkarten 'Verfahrenshistorie' oder 'Anstehendes Verfahren' der Seite **Rechnerübersicht** angezeigt wird.

Anwenden

Klicken Sie auf **Anwenden**, um die ausgewählte Protokollanalyse ausgewählten Rechner-IDs zuzuweisen.

Löschen

Klicken Sie auf **Löschen**, um die ausgewählte Protokollanalyse auf ausgewählten Rechner-IDs zu löschen.

Alle löschen

Klicken Sie auf **Alle löschen**, um alle Protokollanalysen von ausgewählten Rechner-IDs zu entfernen.

Neu...

Wählen Sie `<Select Log Parser>` in der Dropdown-Liste **Protokolldateianalyse** aus und klicken Sie auf **Neu...** *(siehe 359)*, um eine neue Protokollanalyse zu erstellen.

Bearbeiten...

Wählen Sie eine vorhandene Protokollanalyse in der Dropdown-Liste **Protokolldateianalyse** aus und

klicken Sie auf **Bearbeiten...** *(siehe 359)*, um die Protokollanalyse zu bearbeiten.

Protokollanalyse hinzufügen/Protokollanalyse ersetzen

Wählen Sie **Protokollanalyse hinzufügen** aus, um eine Protokollanalyse zu vorhandenen Rechner-IDs hinzuzufügen. Wählen Sie **Protokollanalyse ersetzen** aus, um eine Protokollanalyse hinzuzufügen und alle anderen Protokollanalysen auf den ausgewählten Rechner-IDs zu entfernen.

Definition des Protokolldatei-Parsers

Monitor > Protokoll-Monitoring > Protokollanalyse > Definition der Protokolldateianalyse

Auf der Seite **Definition der Protokolldateianalyse** können Sie Vorlagen und Parameter zur Verwendung mit Analyseprotokolldateien definieren. Die Definitionen werden anschließend über die Seite **Protokollanalyse** *(siehe 357)* den Rechner-IDs zugewiesen. Protokollanalysen sind zunächst zwar privat, können jedoch mit anderen Benutzern gemeinsam verwendet werden.

Der Protokolldateianalysezyklus

Die Analyse einer Protokolldatei wird bei jeder Änderung der Protokolldatei ausgelöst. In den meisten Fällen bedeutet dies das Anhängen von neuem Text an das Ende der Datei. Um zu vermeiden, dass bei jeder Aktualisierung der Datei die gesamte Protokolldatei von Anfang an gescannt wird, parst der Agent Protokolldateien wie folgt:

- Der Agent speichert nach jeder Aktualisierung ein "Lesezeichen" der letzten 512 Byte einer Protokolldatei.
- Wird die Protokolldatei erneut aktualisiert, vergleicht der Agent das Lesezeichen der alten Aktualisierung mit der *gleichen Byteposition* in der neuen Aktualisierung.
- Da Protokolldateien eventuell vor Ausführen der Protokollanalyse archiviert werden, kann die Analyse auch Archivdateien einschließen, sofern vorhanden.
- Durch Angabe vollständiger Pfadnamen mit Sternchen (*) und Fragezeichen (?) als Stellvertreterzeichen können Sie bestimmte Sätze von Protokoll- und Archivdateien festlegen. Wenn ein Satz von Dateien angegeben wurde, beginnt der Parser mit der letzten Datei in dem Satz.
- Wenn der Lesezeichentext in der alten und neuen Aktualisierung identisch ist, beginnt der Agent mit der Analyse des Texts *nach dem Lesezeichen*.
- Falls der Lesezeichentext in den beiden Versionen *nicht* identisch ist und kein Protokollarchivpfad angegeben wurde, analysiert der Agent die gesamte Protokolldatei von Anfang an. Falls ein Protokollarchivpfad angegeben wurde, sucht der Agent in den Archivdateien nach dem Lesezeichen. Wenn das Lesezeichen nicht auffindbar ist, markiert der Agent das Ende der Protokolldatei und beginnt beim nächsten Zyklus an diesem Punkt mit der Analyse.
- Sobald die Analyse abgeschlossen ist, wird ein neues Lesezeichen basierend auf den letzten 512 Byte der neu aktualisierten Protokolldatei definiert und der Prozess wiederholt sich.

> **Hinweis:** Die Analyse einer Protokolldatei selbst gilt nicht als Verfahrensereignis. Nur eine erneute Konfiguration oder Neukonfiguration unter Verwendung von **Protokollanalyse**, **Analysesätze zuweisen** oder **Analyseübersicht** generiert ein Verfahren, das auf den Registerkarten 'Verfahrenshistorie' oder 'Anstehendes Verfahren' der Seite **Rechnerübersicht** angezeigt wird.

Speichern

Wählen Sie **Speichern** aus, um Änderungen an einer Definition der Protokolldateianalyse zu speichern.

Speichern unter...

Wählen Sie **Speichern unter...** aus, um Änderungen an einer Definition der Protokolldateianalyse unter einem anderen Namen zu speichern.

Löschen

Wählen Sie **Löschen** aus, um eine Definition der Protokolldateianalyse zu löschen.

Freigabe....

Sie können Ihre eigenen Definitionen der Protokolldateianalyse mit anderen **VSA-Benutzern** *(siehe 409)* oder **Benutzerrollen** *(siehe 414)* gemeinsam verwenden oder dieses Verfahren allen Benutzern öffentlich zu Verfügung stellen.

Parsername

Geben Sie den Namen der Analyse ein.

Pfad der Protokolldatei

Geben Sie den vollständigen UNC-Pfadnamen oder den Pfadnamen des abgebildeten Laufwerks auf dem Zielrechner der zu analysierenden Protokolldatei ein. Sie können Sternchen (*) oder Fragezeichen (?) als Stellvertreterzeichen verwenden, um einen Satz von Protokolldateien anzugeben. Wenn ein Satz von Protokolldateien angegeben wurde, beginnt die Protokollanalyse mit der letzten Datei in dem Satz. Beispiel: `\\morpheus\logs\message.log` oder `c:\logs\message.log`. Stellen Sie beim Angeben eines UNC-Pfads für eine Freigabe, auf die von einem Agent-Rechner zugegriffen wird – zum Beispiel `\\machinename\share` – sicher, dass die Berechtigung der Freigabe Lese-/Schreibzugriff unter Verwendung der Anmeldedaten für diesen Agent-Rechner in > **Anmeldedaten einstellen** *(siehe 77)* zulässt.

Pfad des Protokollarchivs

Geben Sie den vollständigen UNC-Pfadnamen oder den Pfadnamen des abgebildeten Laufwerks auf dem Zielrechner der zu analysierenden Archivdateien ein. Sie können Sternchen (*) oder Fragezeichen (?) als Stellvertreterzeichen verwenden, um einen Satz von Archivdateien anzugeben. Wenn ein Satz von Archivdateien angegeben wurde, beginnt die Protokollanalyse mit der letzten Datei in dem Satz. Beispiel: Wenn `message.log` täglich in einer Datei mit dem Format `messageYYYYMMDD.log` archiviert wird, können Sie `c:\logs\message*.log` angeben. Stellen Sie beim Angeben eines UNC-Pfads für eine Freigabe, auf die von einem Agent-Rechner zugegriffen wird – zum Beispiel `\\machinename\share` – sicher, dass die Berechtigung der Freigabe Lese-/Schreibzugriff unter Verwendung der Anmeldedaten für diesen Agent-Rechner in > **Anmeldedaten einstellen** *(siehe 77)* zulässt.

Beschreibung

Geben Sie eine Beschreibung für die Protokollanalyse ein.

Vorlage

Anhand dieser Vorlage können Sie die Eingabe mit dem Protokolleintrag in der Protokolldatei vergleichen, um die erforderlichen Daten in Parameter zu extrahieren. Parameter sind in der Vorlage in $-Zeichen eingeschlossen.

Geben Sie ein Muster von Text und Protokolldateiparametern ein. Anhand dieses Muster können Sie vom Beginn jeder Zeile in einer Protokolldatei suchen. Wenn das Muster eine Übereinstimmung in der Protokolldatei findet, werden die Protokolldateiparameter mit den aus der Protokolldatei extrahierten Werten ausgefüllt.

Sie können ein Prozentzeichen (%) als Stellvertreterzeichen verwenden, um eine alphanumerische Zeichenfolge beliebiger Länge anzugeben. Protokolldateiparameter sind in Dollar-Zeichen ($) eingeschlossen. Geben Sie $$ ein, um eine Entsprechung für ein Textmuster zu finden, das ein $-Zeichen enthält. Geben Sie %% ein, um eine Entsprechung für ein Textmuster zu finden, das ein %-Zeichen enthält.

> **Hinweis:** In Vorlagentextmustern muss *die Groß-/Kleinschreibung beachtet werden.*

Beispiel

- Protokolltext: `126 Oct 19 2007 12:30:30 127.0.0.1 Device0[123]: return error code -1!`
- Vorlage: `$EventCode$ $Time$ $HostComputer$ $Dev$[$PID$]:%error code $ErrorCode$!`
- Analysiertes Ergebnis:
  ```
  EventCode=126
  Time= 2007/10/19 12:30:30 Friday
  HostComputer=127.0.0.1
  Dev=Device0
  PID=123
  ErrorCode=-1
  ```

Richtlinien

- So geben Sie ein Tabulatorzeichen in das Bearbeitungsfeld der Vorlage ein:
  1. Kopieren Sie das Tabulatorzeichen in den Protokolldaten und fügen Sie es ein.
  2. Verwenden Sie {tab}, um das Zeichen manuell einzugeben.
- Die einfachste Möglichkeit, eine Vorlage zu erstellen, ist, den Originaltext in die Vorlage zu kopieren und dann die Zeichen, die ignoriert werden können, durch % zu ersetzen. Anschließend ersetzen Sie die Zeichen, die in einem Parameter gespeichert werden, durch einen Parameternamen.
- Achten Sie darauf, dass alle Parameter in der Vorlage in **Protokolldateiparameter** definiert wurden.
- Ein Datum/Uhrzeit-Parameter muss sowohl Datums- als auch Uhrzeitinformationen aus den Quelldaten enthalten, andernfalls verwenden Sie einfach einen Zeichenfolgen-Parameter.

Überspringen von Zeichen

Verwenden Sie zum Überspringen von Zeichen `$[n]$`, wobei `n` die Anzahl der zu überspringenden Zeichen ist. Verwenden Sie `$var[n]$`, um eine feste Anzahl an Zeichen als Variablenwert abzurufen.

Beispiel

- Protokolltext: `0123456789ABCDEFGHIJ`
- Vorlage: `$[10]$ABC$str[3]$`
- Das Ergebnis für den Parameter `str` ist `DEF`.

Multilayer-Vorlage

Wenn diese Option aktiviert ist, werden mehrere Zeilen mit Text und Protokolldateiparameter für die Analyse der Protokolldatei verwendet.

> **Hinweis:** Die Zeichenfolge `{tab}` kann als Tabulatorzeichen und `{nl}` kann als Zeilenumbruch verwendet werden. `{nl}` kann nicht in einer einzeiligen Vorlage verwendet werden. `%` kann als Platzhalterzeichen verwendet werden.

Ausgabevorlage

Geben Sie ein Muster von Text und Protokolldateiparametern ein, die in **Protokoll-Monitoring** gespeichert werden.

Beispiel:

- Ausgabevorlage: `Received device error from $Dev$ on $HostComputer$. Code = $ErrorCode$.`
- Ausgegebenes Ergebnis: `Received device error from Device0 on 127.0.0.1. Code = -1.`

Anwenden

Klicken Sie auf **Anwenden**, um einen in das Feld **Name** eingegebenen Parameter hinzuzufügen oder zu aktualisieren.

Alle löschen

Klicken Sie auf **Alle löschen**, um alle Parameter von der Parameterliste zu löschen.

Protokolldateiparameter

Name

Nachdem Sie die Vorlage erstellt haben, müssen Sie die Liste der Parameter definieren, die von der Vorlage verwendet werden. Alle Parameter in der Liste müssen definiert werden, andernfalls gibt die Analyse einen Fehler zurück. Verfügbare Parameter sind *integer, unsigned integer, long, unsigned long, float, double, datetime, string.* Die Länge des Parameternamens ist auf 32 Zeichen beschränkt.

Geben Sie den Namen eines Parameters ein, der zum Speichern eines Werts verwendet wird. Parameter werden anschließend in den Textfeldern **Vorlage** und **Ausgabevorlage** verwendet.

> **Hinweis:** Schließen Sie den Namen des Parameters im Feld **Name** *nicht* in $-Zeichen ein. Dieses wird nur benötigt, wenn der Parameter in die Textfelder **Vorlage** und **Ausgabevorlage** eingegeben wird.

Typ

Geben Sie den korrekten Datentyp für den Parameter ein. Wenn die in einer Protokolldatei analysierten Daten nicht unter diesem Datentyp gespeichert werden können, bleibt der Parameter leer.

Datumsformat

Wenn als **Typ** die Option `Date Time` ausgewählt wird, geben Sie ein **Datumsformat** ein.

- `yy, yyyy, YY, YYYY` – Zwei- oder vierstelliges Jahr
- `M` – Ein- oder zweistelliger Monat
- `MM` – Zweistelliger Monat
- `MMM` – Abkürzung des Monatsnamens, z. B. "Jan"
- `MMMM` – Vollständiger Monatsname, z. B. "Januar"
- `D, d` – Ein- oder zweistelliger Tag
- `DD, dd` – Zweistelliger Tag
- `DDD, ddd` – Abkürzung des Wochentagsnamens, z. B. "Mon"
- `DDDD, dddd` – Vollständiger Wochentagsname, z. B. "Montag"
- `H, h` – Ein- oder zweistellige Stunde
- `HH, hh` – Zweistellige Stunde
- `m` – Ein- oder zweistellige Minute
- `mm` – Zweistellige Minute
- `s` – Ein- oder zweistellige Sekunde
- `ss` – Zweistellige Sekunde
- `f` – Ein- oder zweistelliger Bruchteil einer Sekunde
- `ff` – fffffffff – zwei bis neun Ziffern
- `t` – Einstellige Zeitmarkierung, z. B. "a"
- `tt` – Zweistellige Zeitmarkierung, z. B. "am"

> **Hinweis:** *Die Datums- und Uhrzeitfilterung in Ansichten und Berichten basiert auf der Uhrzeit des Protokolleintrags*. Bei Einschluss eines Parameters `$Time$` mit dem Datentyp `Date Time` in Ihre Vorlage verwendet das **Protokoll-Monitoring** die im Parameter `$Time$` gespeicherte Zeit als Uhrzeit des Protokolleintrags. Falls *kein* Parameter `$Time$` in Ihre Vorlage eingeschlossen ist, dient die Zeit, zu der der Eintrag in das **Protokoll-Monitoring** hinzugefügt wurde, als Uhrzeit des Protokolleintrags. Jeder Datum/Zeit-Parameter muss mindestens Daten für Monat, Tag, Stunde und Sekunde enthalten.

Beispiel:

- Datum/Zeit-Zeichenfolge: `Oct 19 2007 12:30:30`
- DateTime-Vorlage: `MMM DD YYYY hh:mm:ss`

UTC-Datum

Mit **Protokoll-Monitoring** werden alle Datum/Zeit-Werte als **koordinierte Weltzeit (universal time, coordinated – UTC)** gespeichert. Auf diese Weise können UTC-Datums-/Zeitangeben automatisch in die lokale Zeit des Benutzers konvertiert werden, wenn **Protokollkontroll**daten angezeigt oder Berichte generiert werden.

Wenn diese Angabe leer gelassen wird, werden die im Protokolldateiparameter gespeicherten Datum/Zeit-Werte von der lokalen Zeit der Rechner-ID, die der Protokollanalyse zugewiesen ist, in UTC konvertiert. Wenn diese Option aktiviert ist, liegen die im Protokolldateiparameter gespeicherten Datum/Zeit-Werte bereits in UTC vor und es ist keine Konvertierung erforderlich.

Parser-Sets zuweisen

Monitor > Protokoll-Monitoring > Analysesätze zuweisen

Über die Seite **Analysesätze zuweisen** erstellen und bearbeiten Sie Analysesätze und weisen Analysesätze Rechner-IDs zu. Wahlweise wird ein Alarm basierend auf einer Analysesatzzuweisung ausgelöst. Eine Rechner-ID wird nur in den folgenden Fällen im Seitenbereich angezeigt:

- Die Rechner-ID wurde zuvor über Monitor > **Protokollanalyse** *(siehe 357)* einer **Protokolldatei-Analysedefinition** *(siehe 359)* zugewiesen.
- Die gleiche Protokolldatei-Analysedefinition wurde in der Dropdown-Liste **Protokolldateianalyse auswählen** ausgewählt.

> **Hinweis:** Durch Zuweisen eines Analysesatzes zu einer Rechner-ID über diese Seite wird die Protokollanalyse *aktiviert*. Eine Analyse findet statt, wann immer die analysierte Protokolldatei aktualisiert wird.
>
> **Hinweis:** Unter dem ersten Thema der Online-Hilfe können Sie die PDF-Datei **Schrittweise Konfiguration von Protokollanalysen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_logparsers70.pdf#zoom=70&navpanes=0)* herunterladen.

Benachrichtigung

Der Agent erfasst Protokolleinträge und erstellt einen Eintrag im „Protokoll-Monitoring“-Protokoll, basierend auf den im Analysesatz definierten Kriterien, *egal, ob irgendwelche Benachrichtigungsmethoden aktiviert sind oder nicht.* Sie brauchen nicht jedes Mal benachrichtigt zu werden, wenn ein neuer Protokoll-Monitoring-Eintrag erstellt wird. Sie können einfach nach Bedarf **das „Protokoll-Monitoring“-Protokoll überprüfen** *(siehe 369)*.

Analysedefinitionen und Analysesätze

Bei der Konfiguration des **Protokoll-Monitoring** *(siehe 626)* ist es hilfreich, zwischen zwei Arten von

Konfigurationsdatensätzen zu unterscheiden: **Analysedefinitionen** und **Analysesätze**.

Eine **Analysedefinition** wird für Folgendes verwendet:

- Ermitteln der zu analysierenden Protokolldatei
- Auswählen der Protokolldaten basierend auf dem *Format* der Protokolldaten, laut Angabe in einer Vorlage
- Ausfüllen der Parameter mit Protokolldatenwerten
- Wahlweise Formatierung des Protokolleintrags in **Protokoll-Monitoring**

Mit einem **Analysesatz** werden die ausgewählten Daten anschließend *gefiltert*. Basierend auf den *Werten* der ausgefüllten Parameter und der definierten Kriterien kann ein Analysesatz Protokoll-Monitoring-Einträge generieren und optional Meldungen auslösen.

Falls durch den Analysesatz keine Filterung stattfinden würde, würde die Kaseya Server-Datenbank in kürzester Zeit stark anwachsen. Ein Protokolldateiparameter namens $FileServerCapacity$ würde beispielsweise wiederholt mit dem aktuellen Prozentsatz des freien Speicherplatzes auf einem Dateiserver aktualisiert werden. Bis dieser freie Speicherplatz jedoch auf unter 20 % fällt, braucht dies nicht im **Protokoll-Monitoring** aufgezeichnet zu werden und es braucht auch keine Meldung basierend auf diesem Schwellenwert ausgelöst zu werden. Jeder Analysesatz gilt nur für die Analysedefinition, für deren Filterung er erstellt wurde. Für jede Analysedefinition können mehrere Analysesätze erstellt werden. Jeder Analysesatz kann einen separaten Alarm auf jeder Rechner-ID auslösen, der er zugewiesen wurde.

Protokoll-Monitoring, Setup

1. **Protokollanalyse** – Identifizieren Sie eine Protokolldatei, die anhand einer Protokolldatei-Analysedefinition analysiert werden soll. Eine Protokolldatei-Analysedefinition umfasst die Protokolldateiparameter, die zum Speichern der aus der Protokolldatei extrahierten Werte verwendet werden. Anschließend weisen Sie die Protokollanalyse einem oder mehreren Rechnern zu.
2. **Analysesätze zuweisen** – Definieren Sie einen Analysesatz, um Protokollkontrolldatensätze basierend auf den spezifischen in den Parametern gespeicherten Werten zu generieren. *Aktivieren* Sie die Analyse, indem Sie den Analysesatz einer oder mehreren Rechner-IDs zuweisen, denen Sie zuvor diese Protokollanalyse zugewiesen haben. Definieren Sie wahlweise Meldungen.
3. **Analyseübersicht** – Kopieren Sie auf schnelle Weise *aktive* Analysesatzzuweisungen von einem einzelnen Rechner auf andere Rechner-IDs. Definieren Sie wahlweise Meldungen.

So erstellen Sie einen Analysesatz-Alarm:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
2. Legen Sie weitere E-Mail-Parameter fest.
3. Wählen Sie den Analysesatz aus, der hinzugefügt oder ersetzt werden soll.
4. Markieren Sie die Rechner-IDs, auf die der Alarm angewendet werden soll.
5. Klicken Sie auf die Schaltfläche **Apply**.

So brechen Sie einen Analysesatz-Alarm ab:

1. Aktivieren Sie das Kontrollkästchen für die Rechner-ID.
2. Klicken Sie auf die Schaltfläche **Löschen**.

   Die neben der Rechner-ID aufgeführten Meldungsinformationen werden gelöscht.

Meldungsinformationen an E-Mails und Verfahren weiterleiten

Die folgenden Arten von Monitoring-Meldungs-E-Mails können gesendet und formatiert werden:

- **1 – Meldungen zu einer Protokoll-Monitoring-Analyse.**
- **2 – Meldungen zu mehreren Protokoll-Monitoring-Analysen.**
- **3 – Meldung zu einer fehlenden Protokoll-Monitoring-Analyse.**

> **Hinweis:** Durch Ändern dieses E-Mail-Alarmformats wird das Format von **Analysesätze zuweisen** und **Analyseübersicht** geändert.

Die folgenden Variablen können in die formatierten E-Mail-Meldungen eingeschlossen und an Agent-Verfahren weitergegeben werden, die der Meldung zugewiesen sind. Ein ● in einer nummerierten Spalte gibt an, dass eine Variable mit dem Meldungstyp, der dieser Nummer entspricht, verwendet werden kann.

Innerhalb einer E-Mail-Nachricht	Innerhalb eines Verfahrens	Beschreibung	1	2	3
<ad>	#ad#	duration		●	
<um>	#at#	Alarmzeit	●	●	●
<db-view.column>	Nicht verfügbar	Schließen Sie eine **view.column** *(siehe 484)* aus der Datenbank ein. Um beispielsweise den Computernamen des Rechners, der die Meldung generiert hat, in die E-Mail-Nachricht einzuschließen, verwenden Sie <db-vMachine.ComputerName>.	●	●	●
<ec>	#ec#	Ereigniszählung		●	
<ed>	#ed#	Ereignisbeschreibung	●	●	
<gr>	#gr#	Gruppen-ID	●	●	●
<id>	#id#	Rechner-ID	●	●	●
<lpm>	#lpm#	Protokolldateisatz-Kriterien	●	●	●
<lpn>	#lpn#	Name des Protokollanalysesatzes	●	●	●
<lsn>	#lsn#	Name des Protokolldateisatzes	●	●	●
	#subject#	Betreff der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●
	#body#	Textkörper der E-Mail-Nachricht, falls als Antwort auf eine Meldung eine E-Mail gesendet wurde	●	●	●

Alarm erstellen

Wenn diese Option aktiviert ist und eine **Meldungsbedingung** *(siehe 621)* auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > **Dashboard-Liste** *(siehe 251)*, Monitor > **Alarmübersicht** *(siehe 260)* und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes **Agent-Verfahren** *(siehe 92)* zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail-Empfänger

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.

- Die E-Mail-Adresse des gegenwärtig angemeldeten Benutzers wird im Feld **E-Mail-Empfänger** angezeigt. Der Standardwert wird von System > **Voreinstellungen** *(siehe 402)* übernommen.
- Klicken Sie auf **E-Mail formatieren**, um das Popup-Fenster **Meldungs-E-Mail formatieren** einzublenden. In diesem Fenster können Sie die Anzeige der vom System generierten E-Mails bei Auftreten einer Meldungsbedingung formatieren. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden direkt vom Kaseya Server an die in der Meldung angegebene E-Mail-Adresse gesendet. Legen Sie die **Von-Adresse** über System > **Ausgehende E-Mail** *(siehe 446)* fest.

Protokolldateianalyse auswählen

Wählen Sie eine Protokollanalyse aus der Dropdown-Liste **Protokolldateianalyse auswählen** aus, um alle Rechner-IDs auszuwählen, die zuvor über die Seite **Protokollanalyse** *(siehe 357)* dieser Protokollanalyse zugewiesen wurden.

Protokollsätze für die Entsprechung definieren

Klicken Sie nach Auswahl einer Protokollanalyse auf **Bearbeiten** *(siehe 368)*, um einen neuen Analysesatz zu definieren oder einen vorhandenen Analysesatz in der Dropdown-Liste **Protokollsätze für die Entsprechung definieren** *(siehe 368)* auszuwählen.

Warnen, wenn...

Geben Sie die *Häufigkeit* der Analysesatzbedingung an, die zum Auslösen einer Meldung erforderlich ist:

- **Warnen, wenn dieses Ereignis ein einziges Mal eintritt**
- **Meldung, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden>** eintritt.
- **Meldung, wenn dieses Ereignis nicht innerhalb von <N> <Perioden>** eintritt.
- **Zusätzliche Alarme nicht beachten für <N> <Perioden>**.

Hinzufügen/Ersetzen

Klicken Sie auf die Optionsfelder **Hinzufügen** oder **Ersetzen** und anschließend auf **Anwenden**, um den ausgewählten Analysesatz den ausgewählten Rechner-IDs zuzuweisen.

Entfernen

Klicken Sie auf **Löschen**, um alle Analysesätze von ausgewählten Rechner-IDs zu entfernen.

Anwenden

Wendet den ausgewählten Analysesatz auf die markierten Rechner-IDs an.

Löschen

Löscht die Zuweisung eines ausgewählten Analysesatzes auf ausgewählten Rechner-IDs.

Alle löschen

Löscht alle Analysesätze, die ausgewählten Rechner-IDs zugewiesen sind.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Löschen

Klicken Sie auf das Löschen-Symbol neben einem Analysesatz, um dessen Zuweisung zu einer Rechner-ID zu löschen.

Protokollsatznamen

Listet die Namen der dieser Rechner-ID zugewiesenen Analysesätze auf.

ATSE

Der den Rechner-IDs zugewiesene ATSE-Antwortcode:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Verfahren ausführen
- E = **E**-Mail-Empfänger

E-Mail-Adresse

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Intervall

Gibt das Intervall an, das abgewartet werden soll, um festzustellen, ob ein Ereignis eintritt oder nicht.

Dauer

Gilt nur, wenn die Option **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden> eintritt** aktiviert ist. Bezieht sich auf **<N> <Perioden>**.

Wiederherstellen

Gilt nur, wenn die Option **Zusätzliche Alarme übergehen für <N> <Perioden> aktiviert ist**.

Definition des Protokolldateisatzes

Monitor > Protokoll-Monitoring > Analysesätze zuweisen

- Wählen Sie einen Analysesatz aus der Dropdown-Liste Protokolldateianalyse auswählen.
- Wählen Sie anschließend `<New Parser Set>` oder einen vorhandenen Analysesatz aus der Dropdown-Liste Protokollsätze für die Entsprechung definieren aus. Das Popup-Fenster Definition des Protokolldateisatzes wird eingeblendet.

Im Fenster **Definition des Protokolldateisatzes** können Sie Analysesätze definieren. Ein Analysesatz ist eine Liste von Bedingungen, die erfüllt werden müssen, damit ein **Protokollkontroll**-Datensatz erstellt wird Jede Bedingung stellt eine Kombination von Parameter, Operator und Wert dar.

Analysedefinitionen und Analysesätze

Bei der Konfiguration des **Protokoll-Monitoring** *(siehe 626)* ist es hilfreich, zwischen zwei Arten von Konfigurationsdatensätzen zu unterscheiden: **Analysedefinitionen** und **Analysesätze**.

Eine **Analysedefinition** wird für Folgendes verwendet:

- Ermitteln der zu analysierenden Protokolldatei
- Auswählen der Protokolldaten basierend auf dem *Format* der Protokolldaten, laut Angabe in einer Vorlage
- Ausfüllen der Parameter mit Protokolldatenwerten
- Wahlweise Formatierung des Protokolleintrags in **Protokoll-Monitoring**

Mit einem **Analysesatz** werden die ausgewählten Daten anschließend *gefiltert*. Basierend auf den *Werten* der ausgefüllten Parameter und der definierten Kriterien kann ein Analysesatz Protokoll-Monitoring-Einträge generieren und optional Meldungen auslösen.

Falls durch den Analysesatz keine Filterung stattfinden würde, würde die Kaseya Server-Datenbank in kürzester Zeit stark anwachsen. Ein Protokolldateiparameter namens $FileServerCapacity$ würde beispielsweise wiederholt mit dem aktuellen Prozentsatz des freien Speicherplatzes auf einem Dateiserver aktualisiert werden. Bis dieser freie Speicherplatz jedoch auf unter 20 % fällt, braucht dies nicht im **Protokoll-Monitoring** aufgezeichnet zu werden und es braucht auch keine Meldung basierend auf diesem Schwellenwert ausgelöst zu werden. Jeder Analysesatz gilt nur für die Analysedefinition, für deren Filterung er erstellt wurde. Für jede Analysedefinition können mehrere Analysesätze erstellt werden. Jeder Analysesatz kann einen separaten Alarm auf jeder Rechner-ID auslösen, der er zugewiesen wurde.

So erstellen Sie einen neuen Analysesatz:

1. Geben Sie einen Namen für den Analysesatz ein.
2. Benennen Sie den Analysesatz wahlweise um, indem Sie einen neuen Namen eingeben und auf **Umbenennen** klicken, um die Änderung zu bestätigen.
3. Wählen Sie einen Protokolldateiparameter aus der Dropdown-Liste **Analysespalte**. Protokolldateiparameter werden über die **Definition des Protokolldateisatzes** *(siehe 359)* definiert, die dieser Analysesatz filtern soll.
4. Wählen Sie einen **Operator** aus der Dropdown-Liste. Für verschiedene Datentypen werden verschiedene Listen möglicher Operatoren bereitgestellt.
5. Geben Sie in das Feld **Protokolldateifilter** den gewünschten Wert für den Protokolldateiparameter ein, um einen **Protokollkontroll**-Datensatz zu erstellen.

> **Hinweis:** In Vorlagentextmustern muss *die Groß-/Kleinschreibung beachtet werden.*

6. Klicken Sie auf **Hinzufügen**, um diese Kombination von Parameter/Operator/Wert zu der Liste von Bedingungen hinzuzufügen, die für diesen Analysesatz definiert sind.
7. Klicken Sie auf **Bearbeiten**, um eine vorhandene Kombination von Parameter/Operator/Wert zu zu bearbeiten, und anschließend auf **Speichern**.
8. Klicken Sie auf das Löschen-Symbol ✕, um eine vorhandene Kombination von Parameter/Operator/Wert zu löschen.

Protokoll-Monitoring-Einträge anzeigen

Protokoll-Monitoring-Einträge werden in **Protokoll-Monitoring** angezeigt, die Sie folgendermaßen aufrufen können:

- Agents > **Agent-Protokolle** *(siehe 35)* > Protokoll-Monitoring > (Analysedefinition)
- **Live Connect** *(siehe 393)* > Agent-Daten > Agent-Protokolle > Protokoll-Monitoring > (Analysedefinition) Live Connect kann durch Klicken auf das Check-in-Statussymbol einer ausgewählten Rechner-ID angezeigt werden.
- Inventarisierung > **Rechnerübersicht** *(siehe 151)* > Registerkarte Agent-Protokolle > Protokoll-Monitoring > (Analysedefinition). Die Rechnerübersichtsseite kann auch durch *Alt-Klicken* auf das Check-in-Statussymbol einer ausgewählten Rechner-ID angezeigt werden.
- Der Bericht Info Center > Reporting > Berichte > Monitor – Protokolle > Protokoll-Monitoring.

Kapitel 8

Remote Control

In diesem Kapitel

Fernsteuerung – Überblick

Sie können verwaltete Rechner so anzeigen und bedienen, als ob sie genau vor Ihren Augen wären, indem Sie auf die Rechner-ID klicken. Das Modul **Fernsteuerung** ermöglicht Ihnen Folgendes:

- Automatisches Herstellen einer Verbindung mit dem Remote-Computer, und zwar unabhängig von Gateway- oder Firewall-Konfigurationen, selbst hinter NAT
- Interaktives Arbeiten mit oder auch ohne Benutzer, um Probleme zu lösen, wobei beide Parteien die Geschehnisse in Echtzeit verfolgen können
- Einstellen von Richtlinien, anhand derer Benutzer die Fernsteuerung blockieren können oder vor dem Zugriff auf einen Rechner um Erlaubnis gebeten werden müssen.
- FTP-Zugriff auf jeden verwalteten Rechner und Dateizugriff selbst hinter NAT-Gateways und Firewalls
- Direkter Chat mit jedem verwalteten Rechner. Dies ist perfekt für die Unterstützung von Einwählbenutzern mit nur einer Telefonleitung. Fernsteuerung mit gleichzeitigem Chat ist möglich.
- vPro-aktivierte Rechner hochfahren, herunterfahren, starten und neu starten

Funktionen	Beschreibung
Rechnersteuerung *(siehe 374)*	Erlaubt Benutzern, den Desktop eines verwalteten Rechners anzuzeigen und aus Gründen der Fehlerbehebung und/oder zu Lehrzwecken die Fernsteuerung darüber zu übernehmen.
Passwort zurücksetzen *(siehe 378)*	Setzen Sie das Passwort für ein lokales Konto auf einem verwalteten Rechner zurück.
RC vorinstallieren *(siehe 380)*	Installieren Sie den Fernsteuerungsdienst.
Remote Control deinstallieren *(siehe 381)*	Deinstallieren Sie den Fernsteuerungsdienst.
Benutzerrollen-Richtlinie *(siehe 382)*	Legt fest, wie Rechnerbenutzer darüber benachrichtigt werden, dass eine Fernsteuerungssitzung zu ihrem Rechner bevorsteht. Festgelegt nach VSA-Benutzerrolle.
Rechnerrichtlinie *(siehe 383)*	Legt fest, wie Rechnerbenutzer darüber benachrichtigt werden, dass eine Fernsteuerungssitzung zu ihrem Rechner bevorsteht. Dies wird nach Rechner-ID eingestellt.
FTP *(siehe 385)*	Leiten Sie eine FTP-Sitzung mit einem verwalteten Rechner ein.
SSH *(siehe 387)*	Führt eine SSH-Befehlszeilensitzung auf einem ausgewählten, aktiven Linux- oder Apple-Rechner aus.
Task-Manager *(siehe 388)*	Führt den NT Task Manager remote aus und zeigt Daten im Browser an.
Chat *(siehe 389)*	Startet eine Chat-Sitzung zwischen einem Benutzer und einem Remote-Rechner.
Nachricht senden *(siehe 391)*	Benutzer können Netzwerknachrichten an ausgewählte verwaltete Rechner senden.

Kaseya Remote Control

Kaseya Remote Control ist die primäre Fernsteuerungsfähigkeit, die im gesamten **Virtual System Administrator™** verwendet wird. **Kaseya Remote Control** stellt innerhalb von wenigen Sekunden eine Verbindung zu Remote-Rechnern her, auf denen **Kaseya Remote Control** bereits installiert ist. **Kaseya Remote Control** hält eine zuverlässige, sichere und verschlüsselte Verbindung aufrecht.

Starten von Kaseya Remote Control

Klicken Sie auf ein beliebiges Agent-Symbol, das **Kaseya Remote Control** unterstützt, um es automatisch zu starten bzw. neu zu starten. Sie können auch den Mauszeiger über das Agent-Symbol bewegen, um die **Schnellanzeige** *(siehe 17)* anzuzeigen. Klicken Sie auf die Schaltfläche **Fernsteuerung**, um **Kaseya Remote Control** zu starten.

Hinweis: Sie können **Live Connect** *(siehe 393)* durch Drücken der *Strg-Taste und Klicken* auf das Agent-Symbol starten. Sie können auch auf die **Live Connect**-Schaltfläche in der **Schnellanzeige** klicken.

Installieren und Aktualisieren von Kaseya Remote Control

Kaseya Remote Control ist als Viewer/Serverpaar an Anwendungen installiert: der Viewer auf dem lokalen Rechner des Administrators und der Server auf dem Remote-Agent-Rechner. Der **Kaseya Remote Control**-Server ist als eine Komponente des Agents installiert, wenn ein neuer Agent installiert wird oder wenn der Agent mithilfe von Agent > **Agent aktualisieren** *(siehe 81)* aktualisiert wird.

Wenn die **Kaseya Remote Control**-Anwendung nicht bereits auf Ihrem lokalen Administratorrechner installiert ist, werden Sie beim Start der ersten Sitzung in einem Dialogfeld zum Herunterladen und Installieren aufgefordert. Wenn sie bereits installiert ist und nun eine neuere Version durch eine Kaseya-Patch-Freigabe verfügbar ist, werden Sie in einem Dialogfeld zum Herunterladen und Installieren der aktualisierten Version aufgefordert. Es gibt keinen unabhängigen Start der **Kaseya Remote Control**-Anwendung außerhalb des VSA.

Hauptfunktionen

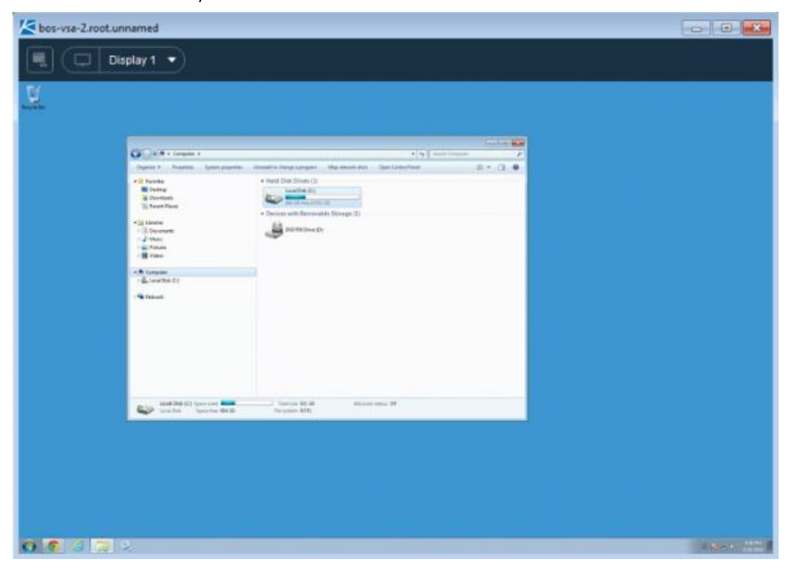
- Unterstützt die Fernsteuerung unabhängig davon, ob ein Rechnerbenutzer angemeldet ist oder nicht.
- Stellt eine Verbindung zur Konsolensitzung her. Ist ein Benutzer angemeldet, gibt der Administrator die Konsolensitzung für den Benutzer frei.
- Ermöglicht dem Administrator, zusätzliche *Monitore* auszuwählen, die möglicherweise auf dem Remote-System laufen.
- Es können mehrere Anzeigesitzungen mit dem gleichen Agent-Rechner verbunden sein und den gleichen oder verschiedene Monitor(e) anzeigen.
- Bewegt *Klartext* durch Kopieren und Einfügen (STRG+C und STRG+V) zwischen lokalen und Remote-Systemen hin und her.
- Unterstützt die Nutzung zahlreicher nativer **Windows- und Apple-Tastenkombinationen** *(https://helpdesk.kaseya.com/entries/58322696)* auf dem Remote-Rechner.
- Verwendet das auf dem Remote-Rechner konfigurierte Tastaturlayout. Die Zeichen auf der lokalen Tastatur des Administrators stimmen möglicherweise nicht mit den auf der Remote-Benutzeroberfläche angezeigten Zeichen überein. Administratoren können das Tastaturlayout auf dem Remote-Rechner vorübergehend ändern, damit es ihrer lokalen Tastatur entspricht. Dies ist eventuell für die Eingabe von Kennwörtern notwendig.
- Stellt eine Verbindung her, wenn ein Windows-Rechner im *abgesicherten Modus mit Netzwerktreibern* gestartet wird.
- Ein Protokolleintrag wird jedes Mal im VSA > System > **Systemprotokoll** *(siehe 442)* erstellt, wenn **Kaseya Remote Control** erfolgreich eine Verbindung zu einer Fernsteuerungssitzung herstellt.

> **Hinweis:** Weiere Informationen finden Sie unter **Kaseya Remote Control-Anforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/Reqs/index.asp#18007.htm)*.

Benutzeroberfläche

Das grundlegende Layout der **Kaseya Remote Control**-Benutzeroberfläche enthält Folgendes:

- Den Rechnernamen, der oberhalb des Fensters der Fernsteuerungssitzung angezeigt wird.
- Eine schmale Menüleiste oben.
- Wird ausschließlich zu Windows-Rechnern eine Verbindung hergestellt, wird die Option "STRG+ALT+DEL senden" für Remote-Anmeldungen in der Menüleiste angezeigt.
- Wenn auf dem Remote-Rechner mehrere Monitore verfügbar sind, wird eine Dropdown-Liste der Monitore angezeigt, aus der ein bestimmter Monitor ausgewählt werden kann.
- Durch Schließen des Fensters wird die Sitzung beendet.
- Die Standard-Bildschirmgröße für ein Sitzungsfenster liegt bei 1280 x 800. Die Standardposition ist mittig auf dem Bildschirm. Für neue Sitzungsfenster werden die Größe und Position verwendet, die zuletzt vom Administrator verwendet wurden.



Entfernte alte Fernsteuerungsfunktionen

In der Version 7.0 wurden alle Funktionen in Zusammenhang mit RADMIN, PC Anywhere, WINVNC, x11vnc Server und UltraVNC-Viewer auf dem Fernsteuerungsmodul entfernt. Die Seiten Fernsteuerung > **Typ auswählen** und **Parameter einstellen** wurden ebenfalls entfernt.

Verwenden von K-VNC

Eine **K-VNC**-Fernsteuerungssitzung kann über die Seite Fernsteuerung > **Kontrollrechner** *(siehe 374)* gestartet werden. Administratoren sollten K-VNC in Situationen nutzen, in denen keine Unterstützung durch **Kaseya Remote Control** vorhanden ist, und in denen eine webbasierte Fernsteuerungslösung erforderlich ist. Die Einstellungen **Sitzungsaufzeichnung** oder **Benutzer benachrichtigen, wenn die Sitzung beendet ist** auf den Seiten **Benutzerrollen-Richtlinie** *(siehe 382)* und **Rechnerrichtlinie** *(siehe 383)* im Modul **Fernsteuerung** werden nur von K-VNC-Fernsteuerungssitzungen unterstützt.

Rechnersteuerung

Fernsteuerung > Desktopsteuerung > Kontrollrechner

Auf der Seite **Kontrollrechner** wird eine Fernsteuerungssitzung zwischen dem lokalen Rechner des

Benutzers und einer ausgewählten Rechner-ID aufgebaut. Fernsteuerungssitzungen können nur von einem Windows-basierten Rechner initiiert werden.

Automatische Installation

Wenn K-VNC nicht bereits auf einem Rechner installiert und eine Fernsteuerungssitzung mithilfe von **Kontrollrechner** *(siehe 374)* initiiert ist, wird das Paket automatisch installiert. Die Installation erfordert keinen Neustart. Die automatische Installation nimmt bis zu einer zusätzlichen Minute in Anspruch. Um diese Verzögerung bei der ersten Verwendung zu eliminieren, können Sie K-VNC über **Vorinstallation RC** *(siehe 380)* auf jedem verwalteten Rechner vorinstallieren.

> **Hinweis:** Durch die Deinstallation eines Agents wird K-VNC oder der KBU-Client, KES-Client oder KDPM-Client nicht entfernt. Vor dem Löschen des Agents verwenden Sie Fernsteuerung > **Fernsteuerung deinstallieren** *(siehe 381)*, um K-VNC auf den verwalteten Rechnern zu deinstallieren. Deinstallieren Sie ebenfalls alle Clients des Zusatzmoduls.

Fernsteuerung einleiten

Leiten Sie die Fernsteuerung ein, indem Sie auf den Namen des Zielrechners klicken. Symbole neben der ID des verwalteten Rechners zeigen den aktuellen Verbindungsstatus dieses Rechners an. Nur Rechner-IDs mit dem Symbol oder oder können eine Verbindung mit Zielrechnern herstellen und über Links verfügen, alle anderen Rechner sind inaktiv.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet. Das Symbol zeigt eine Quickinfo mit dem Anmeldenamen an.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

> **Hinweis:** Benutzer können Fernsteuerungs- und FTP-Sitzungen deaktivieren, indem sie auf das Symbol auf ihrem verwalteten Rechner klicken und **Fernsteuerung deaktivieren** auswählen. Sie können Benutzern diese Fähigkeit verweigern, indem Sie über Agent > **Agent-Menü** *(siehe 66)* die Option **Fernsteuerung deaktivieren** entfernen.

Ausführliche Übertragung aktivieren

Die Fernsteuerung oder FTP von Rechnern hinter Firewalls und NAT-Gateways kann mithilfe einer Hilfsanwendung durch den VSA-Server übertragen werden. Wenn Sie dieses Kontrollkästchen aktivieren, wird ein Popup-Fenster mit Statusinformationen über die normalerweise verborgene Hilfsanwendung angezeigt.

Fernsteuerung des KServers

Wenn Sie auf den Link **KServer** klicken, wird eine Fernsteuerungssitzung mit dem Kaseya Server selbst gestartet. Verwenden Sie diese Funktion, um Ihren Kaseya Server remote zu verwalten. Nur Benutzer mit Master-Rolle können den Kaseya Server fernsteuern.

Fernsteuerung für Rechnerbenutzer

Rechnerbenutzer haben über Agent > **Portalzugriff** *(siehe 75)* Fernzugriff auf ihre Agent-Rechner.

Fernsteuerungs-Fehlfunktionen

Dies sind einige Gründe für eine Fehlfunktion der Fernsteuerung (auf Zielrechnern mit und ohne Agents):

- Der Remote-Rechner blockiert ausgehenden Datenverkehr auf dem Check-in-Port des Agents (Standard 5721). Die Firewall muss eventuell neu konfiguriert werden.
- Der Remote-Rechner verfügt über eine langsame Verbindung. Lassen Sie die Anwendung länger als das Zeitlimit laufen und warten Sie ab, ob dies funktioniert.
- Antiviren-Software auf dem Remote-Rechner kann die Verbindung blockieren. Dieses Problem tritt nicht ein, wenn Endpoint Security-Schutz auf dem Remote-Rechner installiert ist.
- Falsche primäre Kaseya Server-Adresse – Die Fernsteuerung kann nur über die primäre Kaseya Server-Adresse eine Verbindung herstellen. Rechner mit einem Agent können über die Primär- oder Sekundäradresse verbunden werden. Überprüfen Sie mit Agent > **Check-in-Kontrolle** *(siehe 68)*, ob der Remote-Rechner die primäre Kaseya Server-Adresse erkennen kann.

Remote Control in Datei im Arbeitsverzeichnis des Rechners aufzeichnen

Gilt nur für K-VNC. Wenn diese Option aktiviert ist, wird eine **Videoaufzeichnung** *(siehe 617)* einer Fernsteuerungssitzung erstellt.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits
Agent online
Agent online und Benutzer gegenwärtig angemeldet.
Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
Agent ist gegenwärtig offline
Agent hat nie eingecheckt.
Agent ist online, aber die Fernsteuerung wurde deaktiviert.
Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen. Nur Rechner-IDs mit dem Symbol oder oder können eine Verbindung mit Zielrechnern herstellen und über Links verfügen, alle anderen Rechner sind inaktiv.

Aktueller Benutzer

Der gegenwärtig am verwalteten Rechner angemeldete Benutzer

Aktiver Administrator

Der VSA-Benutzer, der gegenwärtig eine Fernsteuerungssitzung zu dieser Rechner-ID ausführt

K-VNC-Symbolleistenoptionen

Eine **K-VNC**-Fernsteuerungssitzung kann über die Seite Fernsteuerung > **Kontrollrechner** *(siehe 374)* gestartet werden. Administratoren sollten K-VNC in Situationen nutzen, in denen keine Unterstützung durch **Kaseya Remote Control** *(siehe 373)* vorhanden ist, und in denen eine webbasierte Fernsteuerungslösung erforderlich ist. Die Einstellungen **Sitzungsaufzeichnung** oder **Benutzer benachrichtigen, wenn die Sitzung beendet ist** auf den Seiten **Benutzerrollen-Richtlinie** *(siehe 382)* und **Rechnerrichtlinie** *(siehe 383)* im Modul **Fernsteuerung** werden nur von K-VNC-Fernsteuerungssitzungen

unterstützt.

Eine K-VNC-Sitzung bietet eine Reihe von Schaltflächen in der Werkzeugleiste zur Verwaltung des Remote-Desktop-Viewers. Bewegen Sie den Mauszeiger über die einzelnen Schaltflächen, um eine Quickinfo anzuzeigen.



- **Optionen festlegen** – Legt Verbindungsoptionen für die aktuelle Viewer-Sitzung fest. Weitere Angaben finden Sie unten.
- **Verbindungsinformationen anzeigen** – Zeigt Verbindungsinformationen zur aktuellen Desktop-Viewer-Sitzung an.
- **Bildschirm aktualisieren** – Aktualisiert die Anzeige des Desktop-Viewers.
- **Verkleinern**
- **Vergrößern**
- **Zoom 100 %**
- **An Fenster anpassen**
- **Vollbild**
- **'Strg-Alt-Entf senden'** – Wählt STRG+ALT+ENTF auf dem Remote-Rechner aus.
- **'Win'-Schlüssel als 'Strg-Esc' senden** – Wählt STRG+ESC auf dem Remote-Rechner aus.
- **Strg-Sperre** – Wenn aktiviert, wird die STRG-Taste auf dem Remote-Rechner gedrückt gehalten.
- **Alt-Sperre** – Wenn aktiviert, wird die ALT-Taste auf dem Remote-Rechner gedrückt gehalten.
- **Trennen**: Trennt die aktuelle Viewer-Sitzung.

Festlegen von Optionen

Format und Kodierungen

Änderungen an diesen Einstellungen gelten nur für die aktuelle Viewer-Sitzung.

- **Bevorzugte Kodierung**
  - `Tight (default)` – In der Regel die beste Wahl für Netzwerkverbindungen mit geringer Bandbreite.
  - `Hextile` – In der Regel die beste Wahl für Netzwerkverbindungen mit hoher Geschwindigkeit.
  - `ZRLE` – Im Applet enthalten, um Kompatibilität mit verschiedenen VNC-Servern herzustellen. Nicht erforderlich in Live Connect.
  - `Raw` – Am schnellsten, wenn sich Server und Viewer auf dem gleichen Rechner befinden.
- **Farbformat** – Reduzierte Farben für eine bessere Leitung bei langsameren Netzwerkverbindungen.
- **Benutzerdefinierter Komprimierungsgrad** – Stufe 1–9. Standardeinstellung ist 6.
  - In Stufe 1 wird die Mindestprozessorzeit verwendet und es werden schwache Komprimierungsverhältnisse erreicht.
  - Für Netzwerkumgebungen mit hoher Bandbreite werden geringere Stufen empfohlen.
  - Stufe 9 bietet die beste Komprimierung, ist aber langsam in Bezug auf den Prozessorzeitbedarf auf dem Remote-Rechner.
  - Für Netzwerkumgebungen mit geringerer Bandbreite werden höhere Stufen empfohlen.
- **JPEG zulassen, Qualitätsstufe festlegen** – Stufe 1–9. Standardeinstellung ist 6.
  - Bezieht sich auf den JPEG-Komprimierungsgrad.
  - Stufe 1 bietet eine schlechte Bildqualität, jedoch höhere Komprimierungsverhältnisse, während Stufe 9 für eine gute Bildqualität bei geringeren Komprimierungsverhältnissen sorgt.
  - Für Netzwerkumgebungen mit geringerer Bandbreite werden niedrigere Stufen empfohlen.

- ➢ Für Netzwerkumgebungen mit hoher Bandbreite werden höhere Stufen empfohlen.
- ➢ Die Deaktivierung wird nur empfohlen, wenn eine perfekte Bildqualität benötigt wird.

- **CopyRect-Kodierung zulassen** – Standardmäßig aktiviert. Spart Bandbreite und Zeit, wenn Teile des Remote-Bildschirms durch Ziehen auf dem Bildschirm bewegt werden.

Einschränkungen

- **Nur Ansicht** – Deaktiviert die Übertragung eines Maus- oder Tastaturvorgangs vom Viewer zum Remote-Rechner.
- **Übertragung der Zwischenablage deaktivieren** – Deaktiviert das Kopieren/Einfügen zwischen dem Viewer und dem Remote-Rechner.

Mauscursor

- **Remote-Cursor lokal verfolgen** – Position des Remote-Cursors wird im Viewer angezeigt.
- **Remote-Server übernimmt Steuerung des Mauscursors** ODER **Remote-Cursor nicht anzeigen** – Position des Remote-Cursors wird im Viewer nicht angezeigt. Spart Bandbreite.

Form des lokalen Cursors

- Wählt die Form des lokalen Cursors aus, wenn sich die Maus über dem Viewer-Fenster befindet.

(Andere)

- **Freigegebene Sitzung anfordern** – Immer aktiviert.

Passwort zurücksetzen

Fernsteuerung > Desktopsteuerung > Passwort zurücksetzen

Auf der Seite **Passwort zurücksetzen** werden ein neues Passwort und gegebenenfalls ein neues Benutzerkonto auf einem verwalteten Rechner erstellt. Hier können außerdem Domain-Benutzerkonten auf Domain-Controllern geändert werden.

Falls der Benutzername noch nicht existiert, aktivieren Sie das Kontrollkästchen **Neues Konto erstellen**, um ein neues Konto mit dem angegebenen Passwort zu erstellen. **Passwort zurücksetzen** gibt einen Fehler aus, wenn Sie versuchen, das Passwort für einen Benutzernamen zurückzusetzen, der noch nicht auf dem verwalteten Rechner erstellt wurde, oder wenn Sie ein Passwort erstellen, das bereits von einem Benutzerkonto verwendet wird. Leere Passwörter sind nicht zulässig.

> **Hinweis:** Um ein Benutzerkonto zu löschen, können Sie ein Verfahren zum Löschen des Kontos erstellen oder es manuell über die Fernsteuerung löschen.

Benutzerpasswort zurücksetzen

Verwenden Sie **Passwort zurücksetzen**, um das Benutzerpasswort in den folgenden Fällen auf allen verwalteten Rechnern zurückzusetzen:

- Ihr Benutzerpasswort ist nicht mehr geheim.
- Ein Mitarbeiter verlässt Ihre Organisation, der das Benutzerpasswort kannte.
- Als Teil einer guten Sicherheitsrichtlinie ist der Zeitpunkt gekommen, das Benutzerpasswort zu ändern.

> **Hinweis:** Auf Nicht-Domain-Controllern wird nur das lokale Benutzerkonto auf dem Remote-Rechner geändert. Auf Domain-Controllern werden durch **Passwort zurücksetzen** die Domain-Benutzerkonten geändert.

Anwenden

Klicken Sie auf **Anwenden**, um Parameter für Passwörter und Benutzerkonten auf ausgewählte Rechner-IDs anzuwenden.

Abbrechen

Klicken Sie auf **Abbrechen**, um anstehende Passwortänderungen und das Erstellen von Benutzerkonten auf ausgewählten Rechner-IDs zu stornieren.

Benutzername

Geben Sie den Benutzernamen auf dem verwalteten Rechner ein.

Neues Konto erstellen

Aktivieren Sie dieses Kontrollkästchen, um ein neues Benutzerkonto auf dem verwalteten Rechner zu erstellen.

als Administrator

Aktivieren Sie dieses Kontrollkästchen, um das neue Benutzerkonto mit Administratorberechtigungen zu erstellen.

Passwort/Bestätigen

Geben Sie ein neues Passwort ein.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Status

Dies ist der Status anstehender Passwortänderungen und Benutzerkontoerstellungen.

RC vorinstallieren

Fernsteuerung > RC konfigurieren > vorinstallieren

Auf der Seite **RC vorinstallieren** können Sie **K-VNC** *(siehe 376)* auf ausgewählten Rechner-IDs installieren, ohne eine Fernsteuerungssitzung einleiten zu müssen. Wenn eine Installation auf einer Rechner-ID ansteht, wird diese Seite automatisch alle 5 Sekunden aktualisiert, bis das Verfahren abgeschlossen ist.

Automatische Installation

Wenn K-VNC nicht bereits auf einem Rechner installiert und eine Fernsteuerungssitzung mithilfe von **Kontrollrechner** *(siehe 374)* initiiert ist, wird das Paket automatisch installiert. Die Installation erfordert keinen Neustart. Die automatische Installation nimmt bis zu einer zusätzlichen Minute in Anspruch. Um diese Verzögerung bei der ersten Verwendung zu eliminieren, können Sie K-VNC über **Vorinstallation RC** *(siehe 380)* auf jedem verwalteten Rechner vorinstallieren.

> **Hinweis:** Durch die Deinstallation eines Agents wird K-VNC oder der KBU-Client, KES-Client oder KDPM-Client nicht entfernt. Vor dem Löschen des Agents verwenden Sie Fernsteuerung > **Fernsteuerung deinstallieren** *(siehe 381)*, um K-VNC auf den verwalteten Rechnern zu deinstallieren. Deinstallieren Sie ebenfalls alle Clients des Zusatzmoduls.

Installieren

Klicken Sie auf **Installieren**, um K-VNC auf ausgewählten Rechner-IDs zu installieren. Linux- und Apple OS X-Agents verwenden nur K-VNC.

Abbrechen

Klicken Sie auf **Abbrechen**, um anstehende Installationsverfahren für ausgewählte Rechner-IDs zu stornieren.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Letzter Status

`Anstehend` deutet an, dass die Installation beim nächsten Einchecken des Rechners beim Kaseya Server ausgeführt wird. Ansonsten wird diese Spalte angezeigt, wenn das Fernsteuerungspaket auf der Rechner-ID installiert wurde.

Remote Control deinstallieren

Fernsteuerung > RC konfigurieren > vorinstallieren

Über die Seite **RC deinstallieren** wird **K-VNC** *(siehe 376)* von ausgewählten Rechner-IDs deinstalliert. Wenn eine Deinstallation auf einer Rechner-ID ansteht, wird diese Seite automatisch alle 5 Sekunden aktualisiert, bis das Verfahren abgeschlossen ist.

Wenn bei einer vorhandenen K-VNC-Installation Probleme auftreten, kann VSA möglicherweise keine K-VNC-Sitzung herstellen. Sollte die Fernsteuerung, die K-VNC verwendet, fehlschlagen, werden durch Ausführung von **RC deinstallieren** bestehende Probleminstallationen auf dieser Rechner-ID bereinigt. Beim nächsten Start einer Fernsteuerungssitzung oder Verwendung von **RC vorinstallieren** *(siehe 380)* wird eine reine Kopie des Fernsteuerungspakets installiert.

> **Hinweis:** Durch die Deinstallation eines Agents wird K-VNC oder der KBU-Client, KES-Client oder KDPM-Client nicht entfernt. Vor dem Löschen des Agents verwenden Sie Fernsteuerung > **Fernsteuerung deinstallieren** *(siehe 381)*, um K-VNC auf den verwalteten Rechnern zu deinstallieren. Deinstallieren Sie ebenfalls alle Clients des Zusatzmoduls.

Deinstallieren

Klicken Sie auf **Deinstallieren**, um das Fernsteuerungspaket von ausgewählten Rechner-IDs zu entfernen.

Abbrechen

Klicken Sie auf **Abbrechen**, um anstehende Deinstallationsverfahren für ausgewählte Rechner-IDs zu stornieren.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Letzter Status

`Pending` deutet an, dass die Installation beim nächsten Einchecken des Rechners beim VSA

ausgeführt wird. Ansonsten wird diese Spalte angezeigt, wenn das Fernsteuerungspaket auf der Rechner-ID deinstalliert wurde.

Benutzerrollen-Richtlinie

Fernsteuerung > Benachrichtigungsrichtlinie > Benutzerrollen-Richtlinie

Auf der Seite **Benutzerrollen-Richtlinie** wird festgelegt, wie Benutzer darüber benachrichtigt werden sollen, dass eine Fernsteuerungssitzung auf ihrem Rechner bevorsteht. Richtlinien werden auf **Benutzerrollen** *(siehe 414)* angewendet.

> **Hinweis:** Informationen über das Anwenden von Benachrichtigungsrichtlinien nach Rechner-ID für die Fernsteuerung finden Sie unter **Rechnerrichtlinien** *(siehe 383)*. Rechnerrichtlinien haben Vorrang vor Benutzerrollen-Richtlinien.

Ausnahmen

K-VNC *(siehe 376)* unterstützt alle Optionen auf dieser Seite. **Kaseya Remote Control** *(siehe 373)* unterstützt alle Optionen auf dieser Seite mit Ausnahme von:

- Benutzer benachrichtigen, wenn die Sitzung beendet ist
- Remote Control in Datei im Arbeitsverzeichnis des Rechners aufzeichnen

Anwenden

Klicken Sie auf **Anwenden**, um Richtlinienparameter auf ausgewählte Rechner-IDs anzuwenden.

Benutzerbenachrichtigungstyp auswählen

- **Automatische Kontrolle –** Dem Benutzer wird nichts mitgeteilt. Sie übernehmen sofort und automatisch die Kontrolle.
- **Meldung, falls der Benutzer angemeldet ist** – Es wird eine Benachrichtigung mit Warntext angezeigt. Der Warntext kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden.
- **Um Erlaubnis fragen, falls der Benutzer angemeldet ist** – Fragen Sie den Benutzer, ob es in Ordnung ist, eine Fernsteuerungssitzung zu beginnen. Der Text dieser Frage kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden. Die Fernsteuerung kann erst beginnen, wenn der Benutzer auf die Schaltfläche **Ja** klickt. Klickt er nach einer Minute auf keine Schaltfläche, wird die Antwort **Nein** angenommen und der VSA entfernt das Dialogfeld vom Zielrechner. Wenn kein Benutzer angemeldet ist, fahren Sie mit der Fernsteuerungssitzung fort.
- **Erlaubnis erforderlich. Verweigert, falls niemand angemeldet ist** – Fragen Sie den Benutzer, ob es in Ordnung ist, eine Fernsteuerungssitzung zu beginnen. Der Text dieser Frage kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden. Die Fernsteuerung kann erst beginnen, wenn der Benutzer auf die Schaltfläche **Ja** klickt. Klickt er nach einer Minute auf keine Schaltfläche, wird die Antwort **Nein** angenommen und der VSA entfernt das Dialogfeld vom Zielrechner. Die Fernsteuerungssitzung wird abgebrochen.

Benutzer benachrichtigen, wenn die Sitzung beendet ist

Nur von K-VNC unterstützt. Aktivieren Sie dieses Kontrollkästchen, um den Benutzer beim Beenden der Sitzung zu benachrichtigen.

Meldung über Sitzungsende

Dies wird nur angezeigt, wenn das Kontrollkästchen **Benutzer benachrichtigen, wenn die Sitzung beendet ist** aktiviert ist. Sie können die Standardmeldung gegebenenfalls abändern. Die Variable `<admin>` ist die einzige Variable, die in dieser Meldung verwendet werden kann.

Warntext der Meldung/Text der Erlaubnisfrage

Dies wird nur angezeigt, wenn für **Benutzerbenachrichtigungstyp auswählen** *nicht* `Silently take control` ausgewählt wurde. Sie können die Standardmeldung gegebenenfalls abändern. Die Variable `<admin>` ist die einzige Variable, die in dieser Meldung verwendet werden kann.

Entfernen

Klicken Sie auf **Entfernen**, um Richtlinienparameter von ausgewählten Rechner-IDs zu entfernen.

Administratormitteilung für Start von Remote Control erforderlich

Aktivieren Sie dieses Kontrollkästchen, damit VSA-Benutzer vor dem Start der Fernsteuerungssitzung eine Anmerkung eingeben müssen. Die Anmerkung ist im Fernsteuerungsprotokoll enthalten und wird dem Rechnerbenutzer nicht angezeigt.

Remote Control in Datei im Arbeitsverzeichnis des Rechners aufzeichnen

Nur von K-VNC unterstützt. Wenn diese Option aktiviert ist, werden Fernsteuerungssitzungen automatisch für Rechner, denen diese Richtlinie zugewiesen ist, **aufgezeichnet** *(siehe 617)*.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Löschen

Klicken Sie auf das Löschen-Symbol ✕ neben einer Benutzerrolle, um die Richtlinie zu löschen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Name der Rolle

Die Liste der **Benutzerrollen** *(siehe 414)*

Richtlinie

Die auf eine Benutzerrolle angewendete Fernsteuerungsrichtlinie

Meldung

Die auf eine Benutzerrolle angewendeten Textmeldungen

Rechnerrichtlinie

Fernsteuerung > Benachrichtigungsrichtlinie > Benutzerrollen-Richtlinie

Auf der Seite **Rechnerrichtlinie** wird festgelegt, wie Benutzer darüber benachrichtigt werden sollen, dass eine Fernsteuerungssitzung auf ihrem Rechner bevorsteht. Diese Richtlinie wird auf **Rechner-IDs** angewendet.

> **Hinweis:** Informationen über das Anwenden von Benachrichtigungsrichtlinien nach Rechner-ID für die Fernsteuerung finden Sie unter **Benutzerrollen-Richtlinie** *(siehe 382)*. Rechnerregeln haben Vorrang vor Benutzerrollen-Richtlinien.

Ausnahmen

K-VNC *(siehe 376)* unterstützt alle Optionen auf dieser Seite. **Kaseya Remote Control** *(siehe 373)* unterstützt

alle Optionen auf dieser Seite mit Ausnahme von:

- Benutzer benachrichtigen, wenn die Sitzung beendet ist
- Remote Control in Datei im Arbeitsverzeichnis des Rechners aufzeichnen

Anwenden

Klicken Sie auf **Anwenden**, um Richtlinienparameter auf ausgewählte Rechner-IDs anzuwenden.

Benutzerbenachrichtigungstyp auswählen

- **Automatische Kontrolle –** Dem Benutzer wird nichts mitgeteilt. Sie übernehmen sofort und automatisch die Kontrolle.
- **Meldung, falls der Benutzer angemeldet ist** – Es wird eine Benachrichtigung mit Warntext angezeigt. Der Warntext kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden.
- **Um Erlaubnis fragen, falls der Benutzer angemeldet ist** – Fragen Sie den Benutzer, ob es in Ordnung ist, eine Fernsteuerungssitzung zu beginnen. Der Text dieser Frage kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden. Die Fernsteuerung kann erst beginnen, wenn der Benutzer auf die Schaltfläche **Ja** klickt. Klickt er nach einer Minute auf keine Schaltfläche, wird die Antwort **Nein** angenommen und der VSA entfernt das Dialogfeld vom Zielrechner. Wenn kein Benutzer angemeldet ist, fahren Sie mit der Fernsteuerungssitzung fort.
- **Erlaubnis erforderlich. Verweigert, falls niemand angemeldet ist** – Fragen Sie den Benutzer, ob es in Ordnung ist, eine Fernsteuerungssitzung zu beginnen. Der Text dieser Frage kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden. Die Fernsteuerung kann erst beginnen, wenn der Benutzer auf die Schaltfläche **Ja** klickt. Klickt er nach einer Minute auf keine Schaltfläche, wird die Antwort **Nein** angenommen und der VSA entfernt das Dialogfeld vom Zielrechner. Die Fernsteuerungssitzung wird abgebrochen.

Benutzer benachrichtigen, wenn die Sitzung beendet ist

Nur von WinVNC unterstützt. Aktivieren Sie dieses Kontrollkästchen, um den Benutzer beim Beenden der Sitzung zu benachrichtigen.

Meldung über Sitzungsende

Dies wird nur angezeigt, wenn das Kontrollkästchen **Benutzer benachrichtigen, wenn die Sitzung beendet ist** aktiviert ist. Sie können die Standardmeldung gegebenenfalls abändern. Die Variable `<admin>` ist die einzige Variable, die in dieser Meldung verwendet werden kann.

Warntext der Meldung/Text der Erlaubnisfrage

Dies wird nur angezeigt, wenn für **Benutzerbenachrichtigungstyp auswählen** *nicht* `Silently take control` ausgewählt wurde. Sie können die Standardmeldung gegebenenfalls abändern. Die Variable `<admin>` ist die einzige Variable, die in dieser Meldung verwendet werden kann.

Entfernen

Klicken Sie auf **Entfernen**, um Richtlinienparameter von ausgewählten Rechner-IDs zu entfernen.

Administratormitteilung für Start von Remote Control erforderlich

Aktivieren Sie dieses Kontrollkästchen, damit VSA-Benutzer vor dem Start der Fernsteuerungssitzung eine Anmerkung eingeben müssen. Die Anmerkung ist im Fernsteuerungsprotokoll enthalten und wird dem Rechnerbenutzer nicht angezeigt.

Remote Control in Datei im Arbeitsverzeichnis des Rechners aufzeichnen

Nur von WinVNC unterstützt. Wenn diese Option aktiviert ist, werden Fernsteuerungssitzungen automatisch für Rechner, denen diese Richtlinie zugewiesen ist, **aufgezeichnet** *(siehe 617)*.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem

Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Löschen

Klicken Sie auf das Löschen-Symbol ✗ neben einer Rechner-ID, um die Richtlinie zu löschen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Richtlinie

Die auf eine Rechner-ID angewendete Fernsteuerungsrichtlinie

Meldung

Die auf eine Rechner-ID angewendeten Textmeldungen

FTP

Fernsteuerung > Dateien/Prozesse > FTP

Auf der Seite **FTP** wird eine FTP-Sitzung zwischen dem lokalen Rechner des Benutzers und einer ausgewählten Rechner-ID aufgebaut. FTP-Sitzungen können nur von einem Windows-basierten Rechner initiiert werden. Sobald dies geschehen ist, wird ein neues Browserfenster mit dem Inhalt einer Festplatte auf dem verwalteten Rechner angezeigt. Sie können Dateien wie gewohnt per Drag & Drop verschieben.

> **Hinweis:** Sie können auch **Live Connect** *(siehe 393)* verwenden, um eine **Dateimanager**-Sitzung mit verwalteten Rechnern je nach unterstütztem Betriebssystemtyp zu initiieren.

Dateiübertragungsprotokoll (File Transfer Protocol, FTP)

File Transfer Protocol (FTP) ist ein häufig verwendetes Protokoll für den Austausch von Dateien über jedes beliebige Netzwerk, dass das TCP/IP-Protokoll unterstützt. Der **FTP-Server** ist das Programm auf der Zielmaschine, das im Netzwerk auf Verbindungsanfragen von anderen Computern achtet. Der **FTP-Client** ist das Programm auf dem lokalen Rechner des VSA-Benutzers, das eine Verbindung zum Server initiiert. Der FTP-Clientrechner erfordert Benutzerzugriffsrechte für den FTP-Serverrechner. Es ist im Lieferumfang des Kaseya Server enthalten und dient hauptsächlich zur Bereitstellung von sofortigem technischem Support. Nach der Verbindung kann der Client Dateien auf den Server hochladen, Dateien vom Server herunterladen, Dateien auf dem Server umbenennen oder löschen usw. Jedes Softwareunternehmen oder jeder einzelne Programmierer kann FTP-Server- oder Clientsoftware erstellen, da das Protokoll ein offener Standard ist. Das FTP-Protokoll wird von praktisch jeder Computerplattform unterstützt. Da Kaseya-FTP-Sitzungen über den Kaseya Server übermittelt werden, sind alle FTP-Sitzungen durch das Kaseya-256-Bit-Protokoll mit Rolling-Code-Verschlüsselung geschützt.

FTP einleiten

Leiten Sie eine FTP-Sitzung ein, indem Sie auf den Namen des Remote-Rechners klicken. Symbole neben der ID des verwalteten Rechners zeigen den aktuellen Verbindungsstatus dieses Rechners an. Nur Rechner-IDs mit dem Symbol oder oder können eine Verbindung mit Zielrechnern

herstellen und über Links verfügen, alle anderen Rechner sind inaktiv.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet. Das Symbol zeigt eine Quickinfo mit dem Anmeldenamen an.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

> **Hinweis:** Benutzer können Fernsteuerungs- und FTP-Sitzungen deaktivieren, indem sie auf das Symbol auf ihrem verwalteten Rechner klicken und **Fernsteuerung deaktivieren** auswählen. Sie können Benutzern diese Fähigkeit verweigern, indem Sie über Agent > **Agent-Menü** *(siehe 66)* die Option **Fernsteuerung deaktivieren** entfernen.

Ausführliche Übertragung aktivieren

Die Fernsteuerung oder FTP von Rechnern hinter Firewalls und NAT-Gateways kann mithilfe einer Hilfsanwendung durch den VSA-Server übertragen werden. Wenn Sie dieses Kontrollkästchen aktivieren, wird ein Popup-Fenster mit Statusinformationen über die normalerweise verborgene Hilfsanwendung angezeigt.

FTP an KServer

Durch Klicken auf den Link **FTP an KServer** wird eine FTP-Sitzung mit dem Kaseya Server selbst gestartet. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

Fähigkeit des Rechnerbenutzers, FTP remote einzuleiten, aktivieren/deaktivieren

Über Agent > **Portalzugriff** *(siehe 75)* und System > **Rechnerrollen** *(siehe 417)* können Benutzer die Fähigkeit des Rechnerbenutzers, FTP remote von einem anderen Rechner zu seinem eigenen Rechner einzuleiten, aktivieren oder deaktivieren.

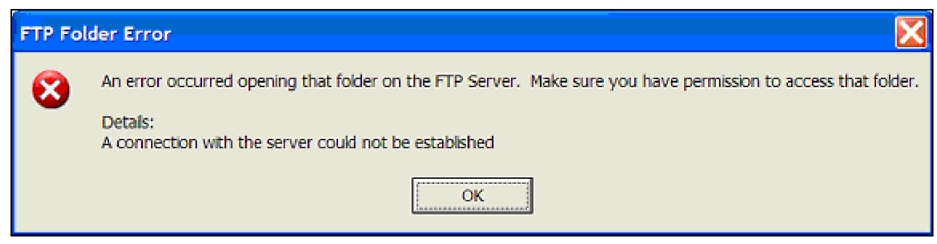
FTP-Fehlfunktionen

Dies sind einige Gründe für FTP-Fehlfunktionen bei verwalteten Rechnern:

- Der Benutzerrechner blockiert ausgehenden Datenverkehr auf dem Check-in-Port des Agents (Standard 5721). Die Firewall muss eventuell neu konfiguriert werden.
- Der Zielrechner verfügt über eine langsame Verbindung. Lassen Sie die Anwendung länger als das Zeitlimit laufen und warten Sie ab, ob dies funktioniert.
- Antiviren-Software auf dem Zielrechner kann die Verbindung blockieren. Dieses Problem tritt nicht ein, wenn KES-Sicherheit auf dem Zielrechner installiert ist.
- Falsche primäre Kaseya Server-Adresse – Die Fernsteuerung kann nur über die primäre Kaseya Server-Adresse eine Verbindung herstellen. Rechner mit einem Agent können über die Primär- oder Sekundäradresse verbunden werden. Überprüfen Sie mit Agent > **Check-in-Kontrolle** *(siehe 68)*, ob der Remote-Rechner die primäre Kaseya Server-Adresse erkennen kann.
- Sie haben von einer anderen Adresse auf den Kaseya Server zugegriffen. Die Hilfsanwendung ruft Verbindungsinformationen von einem Cookie auf dem lokalen Rechner ab. Sie leitet die URL des Kaseya Server an Windows weiter, um auf diese Informationen zuzugreifen. Angenommen, Sie haben die Hilfsanwendung von `www.yourkserver.net` heruntergeladen. Sie öffnen dann einen neuen Browser und greifen auf den Kaseya Server zu, indem Sie seine IP-Adresse `192.168.1.34` eingeben. Der Kaseya Server legt ein Cookie für `192.168.13.34` ab, während die Hilfsanwendung versucht, ein mit `www.yourkserver.net` übereinstimmendes Cookie abzurufen.

Die Hilfsanwendung wird das Cookie nicht finden. Sollte dies geschehen, laden Sie einfach eine neue Hilfsanwendung herunter und probieren es erneut.

- FTP erfordert, dass **Passives FTP deaktiviert** ist. Falls beim Versuch einer FTP-Sitzung der folgende Fehler eintritt:



Deaktivieren Sie wie folgt **Passives FTP** in Ihrem Browser:

1. Öffnen Sie **Internetoptionen...** im Internet Explorer-Menü **Extras**.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Suchen Sie im Abschnitt **Browsen** nach **Passives FTP verwenden** und deaktivieren Sie diese Einstellung.
4. Klicken Sie auf OK und versuchen Sie FTP erneut.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Geben Sie einen Laufwerksbuchstaben für FTP-Übertragung ein

Geben Sie den Laufwerksbuchstaben für die FTP-Übertragung ein, anstatt eine Remote-Festplattenoption auszuwählen.

> **Hinweis:** Der Kaseya Server ermittelt im Verlaufe der **Letzten Inventarisierung** *(siehe 146)*, wie viele Festplatten es auf einem verwalteten Rechner gibt.

SSH

Fernsteuerung > Dateien/Prozesse > SSH

Auf der **SSH**-Seite wird eine SSH-Befehlszeilensitzung auf einem ausgewählten, *aktiven* Linux- oder Apple-Rechner ausgeführt. SSH-Sitzungen können nur über einen Windows-basierten Rechner initiiert werden. Es sind nur Linux- oder Apple-Rechner mit einem -, - oder -Symbol aktiv.

ActiveX-Steuerung

Fernsteuerung, FTP und SSH können nur über Windows OS-Rechner initiiert werden. Das Paket wird automatisch von der ActiveX-Steuerung konfiguriert und ausgeführt. Bei der ersten Verwendung eines dieser Pakete auf einem neuen Rechner werden Sie eventuell vom Browser gefragt, ob es in Ordnung ist, diese ActiveX-Steuerung herunterzuladen und zu installieren. Klicken Sie auf "Ja". Wenn die Ausführung der ActiveX-Steuerung vom Browser blockiert wird, wird dem Benutzer ein Link angezeigt, sodass er das Paket manuell herunterladen und ausführen kann.

Ausführen einer SSH-Sitzung

1. Klicken Sie auf einen beliebigen Linux- oder Mac-Rechner, auf dem ein Hyperlink unterhalb des Rechner-ID-Namens angezeigt wird.
   - Auf einer zweiten Seite wird angegeben, dass die verschlüsselte SSH-Sitzung beginnt.
   - Es wird versucht, die ActiveX-Steuerung automatisch zu laden. Schlägt das Laden einer ActiveX-Steuerung fehl, klicken Sie auf den Hyperlink **hier**, um die ActiveX-Steuerung manuell herunterzuladen und auszuführen.
   - Sobald die ActiveX-Steuerung heruntergeladen und ausgeführt wurde, wird das SSH-Befehlzeilenfenster auf dieser gleichen Seite angezeigt.
2. Sie werden von der SSH-Befehlszeilensitzung dazu aufgefordert, einen Benutzernamen und ein Kennwort des Administrators einzugeben.
3. Klicken Sie auf den Hyperlink **Zurück**, um die SSH-Befehlszeilensitzung zu beenden.

Task-Manager

Fernsteuerung > Dateien/Prozesse > Task Manager

Die Seite **Task Manager** hat dieselbe Funktion wie der Task Manager in Windows NT/2000 von Microsoft. Sie führt alle gegenwärtig aktiven Prozesse auf einem verwalteten Rechner auf. Wenn Sie auf den Link einer Rechner-ID klicken, wird der Agent auf dem verwalteten Rechner beauftragt, beim nächsten Check-in 10 Sekunden an Prozessdaten zu sammeln. Der **Task Manager** zeigt die Ergebnisse als Tabelle an. Der Task Manager unterstützt alle Windows-Betriebssysteme (Windows 95 und höher).

kperfmon.exe

`kperfmon.exe` ist ein kleines Programm, mit dessen Hilfe der Agent Aufgabendaten auf dem Zielrechner sammelt. Es wird nur beim Erfassen der Aufgabendaten ausgeführt. Bei manchen Betriebssystemkonfigurationen kann `kperfmon.exe` während der zur Datenerfassung erforderlichen 10 Sekunden ungefähr 4 % der CPU beanspruchen.

Fähigkeit des Rechnerbenutzers, remote auf den Task Manager zuzugreifen, aktivieren/deaktivieren

Über die Registerkarte System > > Rechnerrollen > **Zugriffsrechte** *(siehe 418)* können VSA-Benutzer den Remote-Zugriff des Rechnerbenutzers auf den Task Manager auf seinem eigenen Rechner von einem anderen Rechner aus aktivieren oder deaktivieren.

Name

Der Name des Prozesses, der aktiv auf dem verwalteten Rechner ausgeführt wird

Prozessor

Der Prozentsatz der Prozessorzeit, die während der zehnsekündigen Datenerfassung von diesem Prozess verbraucht wird

Speichernutzung

Die Menge an Hauptspeicher, die von jedem aktiven Prozess verbraucht wird

Threads

Die Anzahl der mit jedem aktiven Prozess verknüpften aktiven Threads

Prozess beenden

Sie können jeden aktiven Prozess auf dem verwalteten Rechner beenden, indem Sie die Optionsschaltfläche links neben dem Prozessnamen auswählen und dann auf die Schaltfläche **Prozess beenden** klicken. Der aktive Prozess wird beendet und die Aufgabendaten werden erneut gesammelt.

Chat

Fernsteuerung > Mitteilung betrifft Benutzer > Chat

Auf der Seite **Chat** werden Chat-Sitzungen mit anmeldeten Benutzern auf verwalteten Rechnern eingeleitet oder fortgesetzt. Es können mehrere Chat-Sitzungen gleichzeitig aktiv sein. Jeder Fenstertitel zeigt die Rechner-ID für diese Sitzung an. Alle Nachrichten, die älter als eine Stunde sind, werden automatisch vom System entfernt. Drücken Sie die Tastenkombination **Umschalttaste-Eingabe**, um einen Zeilenumbruch in eine Nachricht einzufügen.

> **Hinweis:** Eine Chat- und Video-Chat-Sitzung mit einem verwalteten Rechner kann auch über **Live Connect** *(siehe 393)* eingeleitet werden. Video-Chat lässt Sie über Video mit jeder Person chatten, nicht nur mit dem Benutzer eines verwalteten Rechners.

So leiten Sie eine Chat-Sitzung ein:

Klicken Sie auf die ID des Rechners, mit dem Sie eine Chat-Sitzung einleiten möchten. Ein Chat-Sitzungsfenster wird auf Ihrem Rechner und ein Chat-Fenster in einem Browser auf dem Remote-Rechner geöffnet. Geben Sie Text in das Textfeld ein. Klicken Sie auf die Schaltfläche **Senden**, um die Nachricht zu senden.

So antworten Sie auf eine Chat-Sitzung:

Wenn ein Chat-Popupfenster angezeigt wird, während Sie beim Kaseya Server angemeldet sind, antworten Sie durch Eingabe von Text in das Textfeld. Klicken Sie auf die Schaltfläche **Senden**, um die Nachricht zu senden.

Link "Sitzung beitreten"

Es können mehrere VSA-Benutzer an derselben Chat-Sitzung mit einem Rechnerbenutzer teilnehmen. Wenn eine Chat-Sitzung im Gange ist, wird der Link **Sitzung beitreten** neben der entsprechenden Rechner-ID angezeigt. Klicken Sie auf diesen Link, um der Sitzung beizutreten. **Wurde die Sitzung unregelmäßig beendet**, klicken Sie auf diesen Link, um die Chat-Sitzung neu zu starten und alle Nachrichten für die Sitzung wiederherzustellen.

Chatten mit anderen VSA-Benutzern

Die Namen der **angemeldeten** VSA-Benutzer mit **Umfangs** *(siehe 419)*srechten zu den Organisationen und die Gruppen-IDs, die gegenwärtig vom **Rechner.ID.Gruppen-ID-Filter** *(siehe 626)* aufgelistet werden, werden ebenfalls auf der Seite **Chat** angezeigt. Klicken Sie auf den Link eines anderen angemeldeten VSA-Benutzers, um eine Chat-Sitzung mit diesem VSA-Benutzer einzuleiten.

Aktivieren/Deaktivieren der Fähigkeit des Rechnerbenutzers, Chat mit VSA-Benutzern einzuleiten

Über die Registerkarte System > Rechnerrollen > **Zugriffsrechte** *(siehe 418)* können Benutzer die Fähigkeit des Rechnerbenutzers, eine Chat-Sitzung mit VSA-Benutzern zu initiieren, aktivieren oder deaktivieren.

Sicherstellen, dass Chat ein neues Fenster öffnet

Die Standardeinstellung für **Internet Explorer** verwendet offene Browserfenster neu, wenn eine Aufgabe eine neue URL öffnet. Dies geschieht auch, wenn Sie in einer E-Mail-Nachricht oder einem Word-Dokument auf einen Link klicken (das bereits geöffnete Browserfenster wird an die neue URL umgeleitet). Um das Standardverhalten von Internet Explorer auf das Öffnen von neuen URLs in einem neuen Fenster einzustellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie **Internetoptionen...** im Menü **Extras** eines Internet Explorer-Fensters aus.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Deaktivieren Sie das Kontrollkästchen **Fenster für die Aktivierung von Shortcuts** im Abschnitt "Browsen".
4. Klicken Sie auf **OK**.

Mein Rechner gibt bei jeder Aktualisierung des Chat-Fensters ein "klickendes" Geräusch aus

Viele Windows-Themen konfigurieren das System so, dass jedes Mal ein Ton ausgegeben wird, wenn Internet Explorer zu einer neuen URL navigiert. Einer dieser Töne, `start.wav`, klingt wie ein Klicken. Folgen Sie diesen Schritten, um die Tonwiedergabe zu deaktivieren:

1. Öffnen Sie die **Systemsteuerung** und wählen Sie **Sounds und Multimedia** aus.
2. Klicken Sie auf die Registerkarte **Sounds** .
3. Scrollen Sie nach unten und wählen Sie **Navigation starten** im Abschnitt **Windows Explorer** aus.
4. Wählen Sie in der Dropdown-Liste **Name** die Option **(Keine)** aus.
5. Klicken Sie auf **OK**.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Klang bei jeder neuen Nachricht abspielen

Aktivieren Sie dieses Kontrollkästchen, damit bei jedem Senden oder Empfangen einer neuen Nachricht über ein Chat-Fenster ein Ton ausgegeben wird.

Chatfenster automatisch schließen, wenn einer der Gesprächspartner den Chat beendet

Aktivieren Sie dieses Kontrollkästchen, um das Chat-Fenster zu schließen, wenn eine der Parteien den Chat beendet. Lassen Sie es leer, wenn jeder Partei das Anzeigen und Kopieren von Text aus dem Chat-Fenster möglich sein soll, selbst wenn die andere Partei den Chat beendet.

Entfernen Sie Ihren Namen von der Chatliste, die von anderen Administratoren eingesehen werden kann

Aktivieren Sie dieses Kontrollkästchen, um Ihren Namen aus der von anderen VSA-Benutzern eingesehenen Chat-Liste zu entfernen.

Entfernen Sie Ihren Namen von der Chatliste, die von Benutzern eingesehen werden kann

Aktivieren Sie dieses Kontrollkästchen, um Ihren Namen aus der von Rechnerbenutzern eingesehenen Chat-Liste zu entfernen.

Nachricht senden

Fernsteuerung> Mitteilung betrifft Benutzer > Nachricht senden

Über die Seite **Nachricht senden** können Sie Netzwerknachrichten an ausgewählte Rechner-IDs senden. Die Nachrichten können sofort beim nächsten Check-in des Rechners gesendet oder für einen zukünftigen Zeitpunkt geplant werden.

Die Nachricht wird entweder sofort auf dem verwalteten Rechner angezeigt oder das Agent-Symbol in der Systemablage auf dem verwalteten Rechner blinkt abwechselnd mit einem weißen oder seinem normalen Hintergrund, wenn auf das Lesen der Nachricht gewartet wird. Wenn der Rechnerbenutzer auf das blinkende Symbol klickt, wird die Nachricht angezeigt.

Rechnerbenutzer können auch über ein herkömmliches Windows-Dialogfeld oder ein Browserfenster benachrichtigt werden. Bei Verwendung eines Browserfensters geben Sie eine URL anstelle einer Textnachricht ein. Diese Funktion kann praktisch sein, um beispielsweise Benutzer automatisch zu einer Webseite zu führen, die ein aktualisiertes Kontaktblatt oder sonstige relevante Informationen anzeigt.

Geben Sie die Meldung/URL ein, die an den Remote Rechner gesendet wurde (Dialogfeld oder URL)

Der von Ihnen eingegebene Text hängt vom ausgewählten Anzeigefenster ab.

- Geben Sie eine Textnachricht ein, wenn es sich beim Anzeigefenster um ein Dialogfeld handelt.
- Geben Sie eine URL ein, wenn das Anzeigefenster ein Browser ist.

Anzeigefenster auswählen

Wählen Sie, wie der Benutzer auf dem verwalteten Rechner benachrichtigt wird. Der Standard lautet `Dialog Box`, wodurch ein standardmäßiges Windows-Dialogfeld mit der Netzwerknachricht angezeigt wird. `Browser` zeigt eine URL in einem Webbrowserfenster an.

Jetzt senden

Klicken Sie auf **Jetzt senden**, um die Nachricht sofort an ausgewählte Rechner zu senden. Sie wird in der Spalte **Meldungen noch nicht gesendet** angezeigt, bis sie vom Rechner empfangen wurde. Der Rechner kann beispielsweise offline sein.

Meldungen löschen

Klicken Sie auf **Meldungen löschen**, um Nachrichten zu entfernen, die noch nicht an verwaltete Rechner gesendet wurden.

Zeitpunkt für Versenden der Meldung planen

Geben Sie das Jahr, den Monat, den Tag, die Stunde und Minute zum Senden der Nachricht ein.

Planen

Klicken Sie auf **Planen**, um das Senden der Nachricht unter Verwendung der vorher ausgewählten Planungsoptionen an ausgewählte Rechner zu planen. Die Nachricht wird in der Spalte **Meldungen noch**

nicht gesendet angezeigt, bis sie vom ausgewählten Rechner empfangen wurde.

Sofort anzeigen/Symbol blinken lassen

Mit dieser Einstellung wird festgelegt, wie Benutzer an verwalteten Rechnern nach dem Abrufen ihrer Nachricht vom Kaseya Server benachrichtigt werden.

- Bei Auswahl von **Sofort anzeigen** wird der Benutzer sofort benachrichtigt.
- Bei Auswahl von **Symbol blinken lassen** blinkt das Agent-Symbol in der **Systemablage** *(on seite 631)*, bis der Benutzer auf das Symbol klickt. Die Nachricht wird dann den Einstellungen in **Anzeigefenster auswählen** entsprechend angezeigt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-**Quick View** *(siehe 17)*-Fenster angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits

Agent online

Agent online und Benutzer gegenwärtig angemeldet.

Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

Agent ist gegenwärtig offline

Agent hat nie eingecheckt.

Agent ist online, aber die Fernsteuerung wurde deaktiviert.

Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten **Rechner.Gruppen-IDs** *(siehe 626)* basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > **Scopes** *(siehe 419)* anzuzeigen.

Aktueller Benutzer

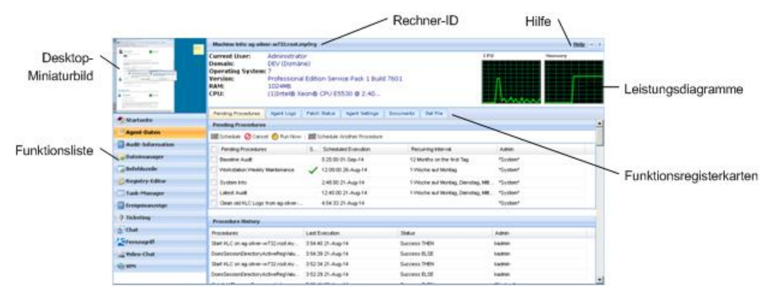
Zeigt den gegenwärtig angemeldeten Benutzer an.

Meldungen noch nicht gesendet

Diese Spalte zeigt die Nachrichten an, die noch nicht gesendet wurden.

Live-Connect

Live Connect ist eine webbasierte, einzelne Rechneroberfläche. Sie können auf **Live Connect** durch Drücken der Strg-Taste und Klicken auf das Agent-Symbol oder durch Klicken auf die Schaltfläche **Live Connect** in der **Schnellansicht** *(siehe 17)* zugreifen. Mithilfe von **Live Connect** können Sie Aufgaben und Funktionen für jeweils einen verwalteten Rechner ausführen. Ein Menü von Eigenschaftenblättern in Form von Registerkarten ermöglicht den Zugriff auf verschiedene Kategorien von Informationen zu dem verwalteten Rechner.



Je nach installierten Zusatzmodulen und dem Betriebssystem des Zielrechners werden weitere Menüelemente angezeigt.

> **Hinweis:** Sowohl das **Live Connect**- als auch das **Portalzugriff**-Plugin-Installationsprogramm kann über die Seite > **Agent aktualisieren** *(siehe 81)* vorinstalliert werden.

Windows

Live Connect für Windows-Rechner unterstützt die folgenden Menüelemente: **Startseite**, **Agent-Daten**, **Audit-Informationen**, **Dateimanager**, **Befehl-Shell**, **Registrierungs-Editor**, **Task Manager**, **Ereignisanzeige**, **Ticketing**, **Chat**, **Desktop-Zugriff** und **Video-Chat**.

> **Plattformübergreifende Unterstützung für Windows-Betriebssysteme:** Unter Windows XP und neueren Systemen können Sie über einen unserer unterstützten Browser die verbesserten Funktionen **Dateimanager**, **Befehls-Shell**, **Registrierungs-Editor**, **Task Manager**, **Ereignisanzeige**, **Desktop-Zugriff** mit Windows XP und neuer verwenden. Unter Mac OS X 10.5 Leopard (Intel) und neueren Systemen können Sie die verbesserten Funktionen **Dateimanager**, **Befehls-Shell** und **Desktop-Zugriff** verwenden.

Apple

Live Connect für Macintosh-Rechner unterstützt die folgenden Menüelemente: **Startseite**, **Agent-Daten**, **Audit-Informationen**, **Dateimanager**, **Befehls-Shell**, **Ticketing**, **Chat**, **Desktop-Zugriff** und **Video-Chat**.

> **Plattformübergreifende Unterstützung für Apple-Betriebssysteme:** Unter Mac OS X 10.5 Leopard (Intel) und neueren Systemen können Sie über einen unserer unterstützten Browser die verbesserten Funktionen **Dateimanager**, **Befehls-Shell**, **Desktop-Zugriff** mit Windows XP und neuer und Mac OS X 10.5 Leopard (Intel) und neueren Systemen verwenden.

Linux

Live Connect für Linux-Rechner unterstützt die folgenden Menüelemente: **Startseite**, **Agent-Daten**, **Audit-Informationen**, **Ticketing**, **Chat** und **Video-Chat**. Bietet keine Bildvorschau im Thumbnailformat auf dem Desktop in **Live Connect**. Verwenden Sie die Seiten **Kontrollrechner** *(siehe 374)*, **FTP** *(siehe 385)* und **SSH** *(siehe 387)*, um Linux-Agents remote zu steuern.

Fensterkopfzeile

Oben im Fenster **Live Connect** werden grundlegende Informationen über den verwalteten Rechner

angezeigt.

- **Miniaturbildansicht** – Der Desktop des gegenwärtig angemeldeten Benutzers wird als Miniaturbild angezeigt, falls ein Benutzer am Rechner angemeldet ist.
- **Rechnerinfo** – Listet grundlegende Informationen über den verwalteten Rechner auf.
- **Leistungsdiagramme** – Zeigt Prozessor- und Speicher-Leistungsdiagramme in Prozent für den verwalteten Rechner an.
- **Abmelden**: Wird nur angezeigt, wenn ein Rechnerbenutzer, der **Portalzugriff** verwendet, remote am Rechner angemeldet ist.
- **Hilfe**: Zeigt die Online-Hilfe für **Live Connect** an.

Menüoptionen

Ein Menü von Eigenschaftenblättern in Form von Registerkarten ermöglicht den Zugriff auf verschiedene Kategorien von Informationen über den verwalteten Rechner.

- **Startseite** – Wenn das Fenster **Live Connect** *geöffnet wird, wird als Erstes die Registerkarte* **Startseite** *angezeigt*.
  - **Startseite** – Normalerweise zeigt die Registerkarte **Startseite** eine Begrüßungsmeldung und die URL-Seite des Agent-Dienstanbieters an. Über den Abschnitt **Verfahren ausführen** der Registerkarte **Startseite** kann der **Live Connect**-Benutzer sofort Agent-Verfahren auf dem verwalteten Rechner ausführen. Falls dies vom Dienstanbieter festgelegt wurde, wird der Abschnitt **Benutzerdefinierte Links** mit Links zu weiteren Ressourcen auf der Registerkarte **Startseite** angezeigt. Es sind mehrere benutzerdefinierte Registerkarten **Startseite** möglich, falls dies vom Dienstanbieter angegeben wurde.
  - **Anmeldenamen ändern** - Ändert den *Remote*-Anmeldenamen und das Passwort des Benutzers für diesen verwalteten Rechner. Anhand dieser Anmeldeoptionen kann ein Benutzer von jedem anderen Rechner auf das Fenster **Live Connect** auf diesem verwalteten Rechner zugreifen und unter Anderem eine Remote-Desktop-Sitzung mit dem verwalteten Rechner einleiten, falls **Desktop-Zugriff** vom Dienstanbieter aktiviert wurde. Geben Sie dieselbe URL ein, die zur Anmeldung beim VSA verwendet wurde. Geben Sie dann den **Live Connect**-Benutzernamen und das Passwort so ein, wie sie auf dieser Registerkarte festgelegt wurden. Diese Methode des Remote-Zugriffs auf **Live Connect** von einem anderen Rechner aus wird als **Portalzugriff** bezeichnet. Anmeldeoptionen für den **Portalzugriff** können auch über Agent > **Portalzugriff** *(siehe 75)* auf dem VSA gepflegt werden.
  - **Profil ändern** – Ändert die Kontaktinformationen für diesen verwalteten Rechner. Wenn **Live Connect** zum Erstellen eines Tickets verwendet wird, wird das Ticket mit diesen Informationen ausgefüllt. Die Informationen können auch über Agent > **Profil bearbeiten** *(siehe 73)* gepflegt werden.
- **Agent-Daten** – Zeigt die folgenden Registerkarten an:
  - **Anstehende Verfahren**: Zeigt und plant anstehende Agent-Verfahren für einen verwalteten Rechner und zeigt die **Verfahrenshistorie** für diesen Rechner an. einschließlich des Datums/der Uhrzeit/des Status der Ausführung und des Benutzers, der das Verfahren plante.
    - ✓ Klicken Sie auf die Schaltfläche **Anderes Verfahren planen**, um ein noch nicht anstehendes Verfahren zu planen. Nachdem das Verfahren ausgewählt und geplant wurde, wird es unten im Abschnitt **Anstehende Verfahren** angezeigt.
    - ✓ Klicken Sie auf die Schaltfläche **Planen**, um ein ausgewähltes Verfahren für die Ausführung zu einem späteren Zeitpunkt oder auf periodischer Basis zu planen.
    - ✓ Klicken Sie auf die Schaltfläche **Jetzt ausführen**, um ein ausgewähltes Verfahren sofort einmal auszuführen.
    - ✓ Klicken Sie auf die Schaltfläche **Abbrechen**, um ausgewählte anstehende Verfahren zu stornieren.
  - **Protokolle** – Zeigt die für diesen Rechner verfügbaren Protokolle an: Alarmprotokoll, Monitoraktionsprotokoll, Agent-Protokoll, Konfigurationsänderungen, Netzwerkstatistiken,

Ereignisprotokoll, Agent-Verfahrensprotokoll, Fernsteuerungsprotokoll, Protokoll-Monitoring.

- **Patch-Status**: Zeigt `Missing` und `Pending` Microsoft-Patches an und plant fehlende Patches. Wenn ein Rechner zu einer **Patch-Richtlinie** *(siehe 624)* gehört, können fehlende Patches außerdem auch als `Denied (Pending Approval)` identifiziert werden. Der Benutzer kann die Patch-Regel "Abgelehnt" manuell außer Kraft setzen, indem er das Patch plant.
  - ✓ Klicken Sie auf den Link **Historie anzeigen**, um die Historie der auf dem verwalteten Rechner installierten Patches anzuzeigen.
  - ✓ Klicken Sie auf die Schaltfläche **Planen**, um die Bereitstellung von fehlenden Patches zu planen.
  - ✓ Klicken Sie auf die Schaltfläche **Jetzt scannen**, um sofort nach fehlenden Patches zu suchen.
  - ✓ Klicken Sie auf die Schaltfläche **Abbrechen**, um ein ausgewähltes anstehendes Patch zu stornieren.
  - ✓ Klicken Sie auf die Schaltfläche **Ignorieren einstellen**, um das Installieren eines Patches über eine der Installationsmethoden zu verhindern. Wird die Installation erforderlich, muss zunächst das Kontrollkästchen **Ignorieren einstellen** deaktiviert werden.
  - ✓ Aktivieren Sie **Patches ausblenden, die von der Patch-Bestätigung abgelehnt wurden**: Wenn diese Option aktiviert ist, werden Patches, die von der Patch-Bestätigung abgelehnt werden, nicht angezeigt.
- **Agent-Einstellungen** – Zeigt Informationen über den Agent auf dem verwalteten Rechner an:
  - ✓ **Agentversion**
  - ✓ **Letzter Check-in**
  - ✓ **Letzter Neustart**
  - ✓ **Erster Check-in**
  - ✓ **Zugehörigkeit zu Patch-Richtlinie** – Wird definiert unter Patch-Verwaltung > Zugehörigkeit: Patch-Richtlinie.
  - ✓ **Definitionskollektionen anzeigen** – Wird über die Option **Nur ausgewählte Rechner-IDs anzeigen** in **Ansichtsdefinitionen** *(siehe 27)* definiert.
  - ✓ **Arbeitsverzeichnis** – Kann auch über "Agent > **Arbeitsverzeichnis** *(siehe 72)*" definiert werden.
  - ✓ **Check-in-Kontrolle** – Kann auch über "Agent > **Check-in-Kontrolle** *(siehe 68)*" definiert werden.
  - ✓ **Profil bearbeiten** – Kann auch über "Agent > **Profil bearbeiten** *(siehe 73)*" definiert werden.
- **Dokumente** – Listet die Dokumente auf, die für einen verwalteten Rechner auf den Kaseya Server hochgeladen wurden. Sie können zusätzliche Dokumente hochladen. Dies stellt dieselbe Funktionalität wie "Audit > **Dokumente** *(siehe 158)*" bereit.
- **Datei abrufen** – Bietet Zugriff auf Dateien, die bereits von einem verwalteten Rechner aus hochgeladen wurden. Klicken Sie auf den Link unterhalb einer Datei, um sie anzuzeigen oder auszuführen. Bietet dieselbe Funktionalität wie Agent-Verfahren > **getFile()** *(siehe 134)*.

▪ **Audit-Informationen** – Die Informationsregisterkarten umfassen: **Rechnerinfo**, **Installierte Anwendungen**, **Systeminformationen**, **Datenträgervolumen**, **PCI & Disk-Hardware**, **Drucker**, **Softwarelizenzen** und **Programme hinzufügen/entfernen**. Stellt Audit-Informationen basierend auf Ihrer **letzten Inventarisierung** *(siehe 615)* zur Verfügung. Über die Registerkarte **Rechnerinfo** können Sie eine sofortige Inventarisierung ausführen.

▪ **Dateimanager** – Zeigt zwei Dateimanager an, einen für den lokalen Rechner und einen anderen für den verwalteten Rechner. In den *oberen Feldern* können Sie Folgendes ausführen:
- Unter Verwendung eines der Dateimanager Verzeichnisse erstellen und löschen, Dateinamen oder Verzeichnisse aktualisieren oder umbenennen
- Dateien unter Verwendung von Drag & Drop im *selben* Dateimanager *verschieben*

- Dateien unter Verwendung von Drag & Drop *zwischen* den Dateimanagern *kopieren*

- **Befehls-Shell** – Öffnet eine Befehls-Shell auf dem verwalteten Rechner. Sie wechselt standardmäßig zum Verzeichnis `c:\windows\system32`.
- **Registrierungs-Editor** – Zeigt die Registrierung der verwalteten Rechner-ID an. Sie können Schlüssel und Werte erstellen, umbenennen, aktualisieren oder löschen sowie Daten für Werte festlegen.
- **Task Manager** – Listet die Daten des Windows-Task Managers für den verwalteten Rechner auf. Sie können **Prozesse** stoppen oder priorisieren, **Dienste** stoppen und starten, nach Prozessor, Platten, Netzwerk und Speicher kategorisierte **Leistungs**-Benchmarks überprüfen, **Benutzer**sitzungsdaten prüfen, den verwalteten Rechner **neu starten** oder herunterfahren oder Sitzungen auf dem verwalteten Rechner abmelden und **Benutzer und Gruppen** auf dem verwalteten Rechner anzeigen. Durch Starten des **Task Manager** können Sie Monitor-Sets mithilfe eines Assistenten basierend auf Prozessen und Diensten erstellen oder ändern. Wenn Sie den Cursor über das Monitorsymbol eines Protokolleintrags bewegen, wird ein Assistent angezeigt.
  - Ein Monitorassistent--Symbol wird neben jedem Prozess und Dienst angezeigt, der in den Registerkarten **Prozesse** und **Dienste** des **Task Manager** aufgelistet ist. Mit diesen beiden Assistenten können Sie ein neues Monitor-Set-Kriterium basierend auf ausgewählten Prozessen oder Diensten aktivieren. Das neue Prozess- oder Dienstkriterium kann zu jedem neuen oder bestehenden Monitor-Set hinzugefügt werden. Das neue oder geänderte Monitor-Set wird sofort auf den Rechner angewendet, der die Quelle dieses Protokolleintrags war. Wird ein bestehendes Monitor-Set geändert, so sind alle Rechner davon betroffen, denen dieses Monitor-Set zugeordnet ist. Unter Monitor > Monitor-Set > **Prozessstatus** *(siehe 274)* und Monitor > Monitor-Set > **Dienstprüfung** *(siehe 273)* finden Sie eine Beschreibung der jeweiligen Felder, die in diesen beiden Assistenten angezeigt werden.
- **Ereignisanzeige** – Zeigt die auf dem verwalteten Rechner gespeicherten Ereignisdaten nach Ereignisprotokolltyp an.
  - Ein Monitorassistent--Symbol wird neben dem Ereignisprotokolleintrag im VSA und in **Live Connect** angezeigt. Wenn Sie den Cursor über das Monitorassistent-Symbol eines Protokolleintrags bewegen, wird ein Assistent angezeigt. Der Assistent ermöglicht Ihnen auf Basis dieses Protokolleintrags ein neues Kriterium für den Ereignissatz zu erstellen. Das neue Ereignissatz-Kriterium kann zu jedem neuen oder bestehenden Ereignissatz hinzugefügt werden. Der neue oder geänderte Ereignissatz wird sofort auf den Rechner angewendet, der die Quelle dieses Protokolleintrags war. Wird ein bestehender Ereignissatz geändert, so sind alle Rechner davon betroffen, denen dieser Ereignissatz zugeordnet ist. Das Monitorassistent-Symbol wird angezeigt in:
    - ✓ Agent > **Agent-Protokolle** *(siehe 35)*
    - ✓ Live Connect > Ereignisanzeige
    - ✓ Live Connect > Agent-Daten > Ereignisprotokoll

    Unter Monitor > **Ereignisprotokoll-Meldungen** *(siehe 316)* finden Sie eine Beschreibung der jeweiligen Felder, die im Assistenten angezeigt werden.
- **Ticketing** – Erstellt Tickets für den verwalteten Rechner und zeigt diese an. Zeigt und erstellt Tickets für **Ticketing**-Modul-Tickets oder Tickets und Knowledge Base-Artikel für das **Service Desk**-Modul, je nachdem, welches Modul aktiviert wurde.

> **Hinweis:** Ein Service-Desk muss Mitglied des Umfangs `Anonymous` sein, um **Service Desk**-Tickets in der **Portalzugriff**-Sitzung von **Live Connect** eines Rechnerbenutzers anzuzeigen.

- **Chat** – Leitet eine Chat-Sitzung mit dem gegenwärtig beim verwalteten Rechner angemeldeten Benutzer ein. Sie können andere VSA-Benutzer zur Teilnahme an der Chat-Sitzung einladen. Weitere Informationen finden Sie unter Fernsteuerung > **Chat** *(siehe 389)*.
- **Fernzugriff** – Leitet eine **Kaseya Remote Control**-Sitzung mit dem verwalteten Rechner ein.

- **Video-Chat** – Wenn ein Rechnerbenutzer an einem verwalteten Rechner angemeldet ist, kann ein **Live Connect**-Benutzer eine Audio-/Video-Chat-Sitzung mit diesem angemeldeten Rechnerbenutzer einleiten. Falls Video nicht auf einem oder beiden Rechnern unterstützt wird, kann die Sitzung für einen oder beide Rechner nur Audio sein.
    - **Video-Chat mit dem Rechnerbenutzer** – Klicken Sie auf die Schaltfläche "Chat", um die Video-Chat-Sitzung einzuleiten. Dem Rechnerbenutzer wird ein Browserfenster oder eine Browserregisterkarte auf seinem Rechner angezeigt, in dem er Ihr Videobild und sein eigenes Videobild sehen kann, wenn eine Webcam auf seinem Rechner installiert ist.
    - **Video-Chat mit jedem** – Klicken Sie auf die Schaltfläche "Verbindungs-URL". Dann wird eine URL in Ihre Zwischenablage kopiert. Kopieren Sie die URL-Adresse in eine E-Mail-Nachricht oder in ein Instant-Messaging-Programm und senden Sie sie an andere Personen. Wenn diese URL in einen Browser eingegeben wird, kann die andere Person einen Video-Chat mit Ihnen halten. *Bei einem Video-Chat ist es nicht erforderlich, dass die Person, die die Chat-Einladung erhält, ein verwalteter Rechner ist.*
    - **Video-Chat-Bestätigung** – Der zur Übertragung des Audio-/Videostroms verwendete Adobe Flash Player erfordert, dass jeder Benutzer auf die Schaltfläche "Zulassen" klickt, um seinerseits mit dem Video-Chat fortzufahren.
    - **Audio-/Videosteuerungen** – Bewegen Sie den Mauszeiger auf eines der Videobilder im Chat-Fenster, um Audio-/Videosteuerungen anzuzeigen.
    - **Text-Chat** – Sie können gleichzeitig einen Text- und Video-Chat im selben Fenster ausführen.
- **VPN** – Nur Windows. Durch Klicken auf diese Option wird eine VPN-Verbindung zwischen dem lokalen Rechner und dem **Live Connect**-Rechner hergestellt. Sobald eine Verbindung hergestellt wurde, kann der Administrator eine Verbindung zu anderen Rechnern herstellen, die das gleiche LAN wie der **Live Connect**-Rechner verwenden, selbst wenn auf diesen Rechnern kein Agent installiert ist. Dies umfasst die Verwendung von Anwendungen, wie SSH oder Telnet, oder das Erstellen anderer Browser-Instanzen, die auf diese anderen Rechner im gleichen LAN abzielen. Die VPN-Sitzung endet, wenn das **Live Connect**-Fenster geschlossen oder die Schaltfläche **VPN anhalten** im **VPN**-Menü ausgewählt wird.
- **AntiMalware** – Zeigt den **AntiMalware**-Status des verwalteten Rechners an, falls installiert.
- **Antivirus** – Zeigt den **Antivirus**-Status des verwalteten Rechners an, falls installiert.
- **Datensicherung** – Wenn **Data Backup** für den verwalteten Rechner aktiviert ist, können Sie dieses Menü verwenden, um:
    - Sicherungen automatisch auszuführen.
    - Ausgewählte Sicherungen, Verzeichnisse und Dateien wiederherzustellen, wenn sie sich auf dem gleichen Rechner befinden.
    - Den Status und die Historie von Sicherungen anzuzeigen.
- **Ermittlung** – Zeigt den **Network Discovery**-Status des Rechners an, falls installiert.

Plugin-Manager

Die verbesserten Funktionen des Browsers von **Live Connect** werden über einen *Plugin-Manager* verwaltet.

- **Plugin-Manager-Installation** – Der Benutzer wird aufgefordert, den Plugin-Manager nach der ersten Anmeldung zu installieren. Die Installation des Plugin-Managers kann hinausgeschoben werden, bis **Live Connect** zum ersten Mal gestartet wird.
- **Plugin-Updates** – IE- und Firefox-Browser erkennen Plugins, die veraltet sind, und laden sie automatisch im Hintergrund herunter. Ein Neustart des Browsers ist für diese beiden Browser nicht erforderlich. Chrome- und Safari-Browser erkennen ebenfalls veraltete Plugins und laden diese im Hintergrund herunter, ohne dass Benutzereingriff erforderlich ist.

Weitere Anmerkungen

- Der Zugriff auf spezifische **Live Connect**-Funktionen hängt von den Zugriffsrechten in System > Benutzerrollen > **Zugriffsrechte** *(siehe 415)* und Rechnerrollen > **Zugriffsrechte** *(siehe 418)* ab.

- Alle **Live Connect** -Menüoptionen sind aktiviert, wenn der Rechner mit **Live Connect** verbunden ist. Wenn der Rechner von **Live Connect** getrennt ist, sind nur **Startseite**, **Audit-Informationen, Agent-Daten** und **Ticketing** aktiviert.
- *Sie können die* **Live Connect-Startseite** *mithilfe von System > Anpassen: Live Connect (siehe 452) anpassen.*
- **Ereignisanzeige**daten sind nicht von Agent > **Ereignisprotokolleinstellungen** *(siehe 38)* abhängig.
- Wenn ein `externalLink.xml` im `\Webpages\install`-Verzeichnis des Kaseya Server vorhanden ist, wird ein **Neues Ticket**-Link neben dem **Hilfe**-Link in **Live Connect** angezeigt. Durch Klicken auf den Link **Neues Ticket** werden die Benutzer auf die in `externalLink.xml` angegebene URL umgeleitet. Weitere Informationen finden Sie unter **Neuen Ticket-Link anpassen** *(siehe 398)*.

Angepasster "Neues Ticket"-Link

Zum Anpassen des Links **Neues Ticket** auf der Seite **Live Connect** tragen Sie die erforderlichen Angaben entsprechend dem Kommentarabschnitt der folgenden XML in die Datei `externalLink.xml` ein. Legen Sie die `externalLink.xml`-Datei zur Aktivierung des neuen Ticket-Links im `\WebPages\install\`-Verzeichnis Ihres Kaseya Server ab.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<externalLinks>
  <!--
  URL STRING SUBSTITUTIONS: The URL string displayed is associated
  with a particular machine ID. The string is searched for the following
  case sensitive values and substituted for the values below.
  machineNameVal - the machine name for the active machine is substituted
                   in the URL string.
  groupNameVal - the group name for the active group.
  -->
  <ticketLink displayName="Ext Ticket"
url="http://192.168.212.52/?mname=machineNameVal&amp;gname=groupNameVal"/>
</externalLinks>
```

Kapitel 9

System

In diesem Kapitel

Systemübersicht

System

Mithilfe des Moduls **System** können Benutzer Regeln für das gesamte System pflegen:

- **Voreinstellungen**
- **Benutzersicherheit**
- **Organisationen, Gruppen, Abteilungen und Mitarbeiter**
- **Serververwaltung**
- **Anpassung**
- **Datenbanksichten**

Funktionen	Beschreibung
Voreinstellungen *(siehe 402)*	Stellt systemweite Präferenzen ein, die nur für den gegenwärtig angemeldeten Benutzer gelten.
Login ändern *(siehe 404)*	Ändert den Benutzernamen, das Passwort und die Sicherheitsfrage des gegenwärtig angemeldeten Benutzers.
Check-in-Richtlinie *(siehe 405)*	Stellt Limits für eine Vielzahl von Parametern für den Agent-Check-in ein.
Benennungsrichtlinie *(siehe 406)*	Erzwingt automatisch Benennungsregeln, die auf der IP-Adresse, dem Netzwerk und dem Computernamen jedes Rechners basieren.
Benutzer *(siehe 409)*	Erstellt, bearbeitet und löscht Benutzer.
Benutzerrollen *(siehe 414)*	Erstellt und löscht Benutzerrollen. Benutzerrollen bestimmen die Zugriffsrechte für VSA-Benutzer. Weisen Sie Rollentypen zu Benutzerrollen zu.
Rechnerrollen *(siehe 417)*	Erstellt und löscht Rechnerrollen. Rechnerrollen bestimmen die Zugriffsrechte für Rechnerbenutzer. Weisen Sie Rollentypen zu Rechnerrollen zu.
Scopes *(siehe 419)*	Weist Organisationen, Rechnergruppen, Rechner, Abteilungen und Service-Desks zu Umfängen zu.
Anmeldezeiten *(siehe 422)*	Gibt an, wann sich Benutzer beim VSA anmelden können.
Benutzerhistorie *(siehe 423)*	Zeigt die Funktionen an, die von jedem Benutzer während der letzten 30 Tage aufgesucht wurden.
Verwalten *(siehe 423)*	Definiert Organisationen, Gruppen, Abteilungen und Mitarbeiter in Abteilungen.
Arten einrichten *(siehe 428)*	Definiert Organisationstypen.
Support anfordern *(siehe 428)*	Greift auf den Kaseya-Support zu.
Konfigurieren *(siehe 429)*	Zeigt Kaseya Server-Informationen, den Lizenzcode und Subskriptionsinformationen an und ruft die aktuellsten Serveraktualisierungen und Server-IP-Informationen ab.
Standard-Einstellungen *(siehe 437)*	Gibt die Standard-Einstellungen für die Serververwaltung an. Gilt für alle **Tenant-Partitionen** *(siehe 631)*.
Lizenzmanager *(siehe 438)*	Weist verfügbare Agent- und Benutzerlizenzen zu.
Import-Center *(siehe 441)*	Importiert und exportiert benutzerdefinierte Automationslösungen in und aus dem VSA.
Systemprotokoll *(siehe 442)*	Protokolliert Ereignisse, die nicht nach Rechner-ID

	verfolgt werden können.
Statistiken *(siehe 442)*	Zeigt Statistiken zur VSA-Serverleistung an.
Anmelderichtlinie *(siehe 444)*	Stellt Anmelderegeln ein.
Anwendungsprotokollierung *(siehe 445)*	Aktiviert oder deaktiviert die Protokollierung von Vorgängen auf Anwendungsebene. Dies wird normalerweise nur vom Kaseya-Support verwendet.
Ausgehende E-Mail *(siehe 446)*	Definiert den E-Mail-Server für ausgehende E-Mail-Nachrichten.
Farbschema *(siehe 15)*	Legt die Farben fest, die von der VSA-Umgebung für den aktuellen Benutzer angezeigt werden.
Seitenanpassung *(siehe 447)*	Passt die Benutzeroberfläche für alle Benutzer an. • Anmeldeseite • Website-Kopfzeile • Berichtskopfzeile • Agent-Symbole
Lokale Einstellungen *(siehe 452)*	Legt **für Tenant-Partitionen spezifische** *(siehe 631)* Einstellungen fest.
Live-Connect *(siehe 452)*	Passt die Live-Connect-Startseiten an, die von VSA-Benutzern und Rechnerbenutzern gesehen werden.
Datenbanksichten *(siehe 479)*	Konfiguriert den Zugriff auf Datenbankansichten.

Anmelderichtlinien für VSA

Nachdem ein VSA-Benutzer über "System > **Benutzersicherheit** *(siehe 408)*" definiert wurde, wird von einer Reihe von Funktionen bestimmt, wann und wie sich Benutzer anmelden können und welche Funktionen ihnen bei der Anmeldung zur Verfügung stehen.

Die bei der Anmeldung für VSA-Benutzer verfügbaren Optionen werden wie folgt festgelegt:

- System > **Benutzer** *(siehe 409)* – Setzen Sie optional das Benutzerpasswort zurück oder zwingen Sie den Benutzer, sein Passwort zu ändern, oder aktivieren/deaktivieren Sie die Benutzeranmeldung oder melden Sie einen Benutzer ab.
- System > **Voreinstellungen** *(siehe 402)* – Auf der Seite **Präferenzen** werden Präferenzoptionen festgelegt, die normalerweise *nur für den gegenwärtig angemeldeten* Benutzer gelten.
- System > **Login ändern** *(siehe 404)* – Auf der Seite **Login ändern** werden Ihr VSA-Benutzername und -Passwort für die Anmeldung festgelegt. Diese Präferenzoptionen gelten *nur für den gegenwärtig angemeldeten* Benutzer.
- System > **Anmelderichtlinie** *(siehe 444)* – Auf der Seite **Anmelderichtlinie** werden für alle VSA-Benutzer gültige Anmelderichtlinien eingerichtet.
- System > **Anmeldezeiten** *(siehe 422)* – Auf der Seite **Anmeldestunden** wird festgelegt, *wann* sich Benutzer beim VSA anmelden können, indem die Wochentage und Stunden für jede Benutzerrolle angegeben werden. Für jeden Tag der Woche können verschiedene Betriebsstunden eingestellt werden.
- System > Seitenanpassung > **Anmeldeseite** *(siehe 448)* – Legen Sie die Optionen fest, die am unteren Rand der Anmeldeseite angezeigt werden.
- System > Seitenanpassung > **Website-Kopfzeile** *(siehe 448)* – Legen Sie die Optionen fest, auf der Anmeldeseite angezeigt werden.

> **Hinweis:** Weitere Anmeldeoptionen *nur für Rechnerbenutzer* werden über "Agent > **Portalzugriff** *(siehe 75)*" eingestellt.

Benutzereinstellungen

Auf den Seiten **Benutzereinstellungen** werden Optionen festgelegt, die normalerweise *nur für den gegenwärtig angemeldeten* Benutzer gelten.

Voreinstellungen

System > Benutzereinstellungen > Voreinstellungen

Auf der Seite **Präferenzen** werden systemweite Präferenzoptionen festgelegt, die *nur für den gegenwärtig angemeldeten* Benutzer gelten. Dazu gehört die E-Mail-Adresse, an der Sie Meldungen empfangen.

Hinweis: Drei Optionen auf dieser Seite gelten für *alle* Benutzer und werden nur für Benutzer mit Master-Rolle angezeigt: Einstellen der **Standardsprache des Systems**, die Schaltfläche **Herunterladen** zum Installieren von Sprachpaketen und **Freigegebene und private Ordnerinhalte aller Benutzer anzeigen**.

Hinweis: Eine Zusammenfassung der Funktionen, die sich auf Benutzeranmeldungen auswirken, finden Sie unter **Anmelderichtlinien für VSA** *(siehe 401)*.

E-Mail-Adresse so einrichten, dass Nachrichten für diesen Administrator gesendet werden an

Gibt die E-Mail-Adresse an, an die Meldungen, Ticketbenachrichtigungen und sonstige E-Mail-Nachrichten gesendet werden. Klicken Sie nach Eingabe der E-Mail-Adresse auf **Anwenden**, um sie aktiv zu machen. Bereits eingestellte Meldungen behalten die ursprünglichen E-Mail-Empfängeradressen, die beim Einstellen der Meldungen angegeben wurden.

Erste Funktion nach Anmeldung einstellen

Wählen Sie den Namen der Funktion, die bei Ihrer ersten Anmeldung beim Kaseya Server angezeigt werden soll.

Verzögerung einstellen, bevor die detaillierten Daten beim Bewegen über ein Informationssymbol angezeigt werden

In jeder Ticketzeile in "Ticketing > **Übersicht anzeigen** *(siehe 457)*" und "Service-Desk > **Tickets** *(http://help.kaseya.com/webhelp/DE/KSD/7000000/index.asp#3646.htm)*" wird ein Informationssymbol angezeigt. Wenn Sie den Cursor darauf bewegen, sehen Sie eine Vorschau des Tickets. Geben Sie die Anzahl der Millisekunden an, die bis zur Anzeige der Ticketvorschau verstreichen sollen, und klicken Sie auf **Anwenden**. Klicken Sie auf die Schaltfläche **Standard**, um diesen Wert auf seinen Standard zurückzusetzen.

Verzögerung einstellen, bevor Daten beim Zeigen auf Agent-Symbol angezeigt werden

Neben jedem Rechner-ID-Konto im wird ein Agent-Check-in-Symbol angezeigt, beispielsweise VSA. Wenn Sie den Cursor darauf bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* geöffnet. Geben Sie die Anzahl der Millisekunden an, die bis zur Anzeige des Agent-Schnellansichtsfensters verstreichen sollen, und klicken Sie auf **Anwenden**. Klicken Sie auf die Schaltfläche **Standard**, um diesen Wert auf seinen Standard zurückzusetzen.

Zeitzonen-Offset auswählen

Wählen Sie eine der folgenden Optionen für den Zeitzonen-Offset aus und klicken Sie dann auf **Anwenden**. Siehe **Zeitplanung und Sommerzeit** *(siehe 403)*.

- **Zeitzone verwenden, mit der sich der Browser am System anmeldet**
- **Zeitzone des VSA-Servers verwenden** – Neben dieser Option wird die Uhrzeit angezeigt, die derzeit in Ihrem VSA-Browser angegeben wird.
- **Festes Offset vom VSA-Server verwenden <N> Stunden**

Hinweis: Das Datumsformat wird unter "System > **Konfigurieren** *(siehe 429)*" eingestellt.

Sprachvoreinstellungen vornehmen

- **Meine Sprachvoreinstellung ist** – Wählen Sie die Sprache aus, die angezeigt werden soll, wenn Sie beim VSA angemeldet sind. Die verfügbaren Sprachen hängen von den installierten Sprachpaketen ab.
- **Die Standardsprachvoreinstellung des Systems ist** – Wählen Sie die Standardsprache aus, die von VSA-Benutzeroberfläche für alle Benutzer verwendet wird. Die verfügbaren Sprachen hängen von den installierten Sprachpaketen ab. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.
- **Sprachpaket herunterladen** – Öffnet ein Dialogfeld, in dem Sie Sprachpakete herunterladen und installieren können. Ein Sprachpaket ermöglicht, dass die VSA-Benutzeroberfläche in dieser Sprache angezeigt wird. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

Freigegebene und private Ordnerinhalte aller Benutzer anzeigen – Nur Hauptadministrator

Wenn dies aktiviert ist, hat ein Benutzer mit Master-Rolle Sichtbarkeit aller freigegebenen und privaten Ordner. Dies gilt nur für private Ordner: Das Aktivieren dieses Kontrollkästchens verleiht dem Benutzer mit Master-Rolle genau wie dem Eigentümer sämtliche Zugriffsrechte.

Anzeigeformat für lange Namen auswählen

Die Webseiten sind für eine gute Anzeige typischer Zeichenfolgenlängen ausgelegt. Gelegentlich enthalten die Datenfelder lange Namen, die nicht richtig auf den Webseiten angezeigt werden. Sie können wie folgt festlegen, wie lange Namen angezeigt werden:

- **Namen für eine bessere Seitengestaltung beschränken** – Diese Einstellung beschränkt die Zeichenfolgenlänge, sodass sie gut auf die Webseite passt. Zeichenfolgen, die eine maximale Länge überschreiten, werden mit .. begrenzt. Wenn Sie den ganzen Namen anzeigen möchten, setzen Sie den Mauszeiger auf die Zeichenfolge. Dann wird ein Tooltip mit dem ganzen Namen angezeigt.
- **Trennen langer Namen zulassen** – Es wird gestattet, dass lange Zeichenfolgen auf der Webseite getrennt werden. Dies kann die normale Gestaltung der Webseite stören und Namen können an jeder Zeichenposition getrennt werden.

Sparmodus löschen

Klicken Sie auf **Sparmodus löschen**, um alle Benachrichtigungen zu ausstehenden Aufgaben zu löschen. Aufgabenbenachrichtigungen werden für Ihnen zugewiesene Aufgaben und Aufgaben, deren Fälligkeitsdatum abgelaufen ist, erzeugt. Aufgaben werden auf der Seite "Infocenter > **Dashboard anzeigen** *(siehe 241)*" definiert.

Standardeinstellungen

Klicken Sie auf **Standards**, um alle Einstellungen für diesen Benutzer auf den Systemstandard zurückzusetzen.

Zeitplanung und Sommerzeit

Der VSA passt die Uhrzeit geplanter Ereignisse beim Übergang zwischen Winter- und Sommerzeit nicht automatisch an. Bei der Planung einer Aufgabe wird die dabei verwendete Zeitzone in die Uhrzeit des Kaseya-Servers konvertiert. Unabhängig der vom Benutzer voreingestellten Zeitzone unter "System >Voreinstellungen" bzw. unabhängig davon, ob die **Zeitplanung nach Agent-Zeit** *(siehe 624)* verwendet wird oder nicht, gilt für die Aufgaben nach der Planung nur mehr die Kaseya-Serverzeit.

Dieses Problem kann folgendermaßen umgangen werden:

- **Systemuhr des Kaseya-Servers verwenden** – *Nur vor Ort* – Wenn die Systemuhr des Hostsystems des Kaseya-Servers für die Umstellung auf die Sommerzeit konfiguriert ist, werden VSA-Aufgaben automatisch angepasst. Diese Option ist bei SaaS nicht verfügbar, da in in derselben Instanz

mehrere Mandanten aus verschiedenen Ländern und Zeitzonen gehostet werden. Die Umstellung auf Sommerzeit ist länderabhängig. SaaS-Instanzen sind auf Greenwich Mean Time (GMT) eingestellt und werden nie geändert.

- **Einmal planen** – *Vor Ort und SaaS* – Die einfachste Methode für den Umgang mit Winter- und Sommerzeit besteht darin, die Zeitpläne einmal festzulegen und sie eine Stunde früher oder später auszuführen, je nachdem ob sie mit Winter- oder Sommerzeit festgelegt wurden.   Da in Mitteleuropa die Sommerzeit länger dauert als die Winterzeit (7 von 12 Monaten), empfiehlt sich für Mitteleuropa die Zeitplanung nach Sommerzeit.

Login ändern

System > Benutzereinstellungen > Login ändern

Auf der Seite **Login ändern** werden Ihr VSA-Benutzername und -Passwort für die Anmeldung festgelegt. Diese Präferenzoptionen gelten *nur für den gegenwärtig angemeldeten* Benutzer.

> **Hinweis:** Eine Zusammenfassung der Funktionen, die sich auf Benutzeranmeldungen auswirken, finden Sie unter **Anmelderichtlinien für VSA** *(siehe 401)*.

Anmeldenamen und/oder Passwort für VSA ändern

So ändern Sie Ihren Anmeldenamen und Ihr Passwort:

1. Geben Sie einen neuen Namen in das Feld **Benutzername** ein.

   > **Hinweis:** Das Feld **Benutzername** kann nicht bearbeitet werden, wenn die Option **Verhindern, dass Benutzer ihre Anmeldedaten ändern** unter **System > Anmelderichtlinie** aktiviert ist.

2. Geben Sie Ihr altes Passwort in das Feld **Altes Passwort** ein.
3. Geben Sie ein neues Passwort in das Feld **Neues Passwort** ein. Bei Passwörtern muss die Groß-/Kleinschreibung beachtet werden.

   Hinweis: Wenn Sie möchten, dass das System ein starkes Passwort für Sie erzeugt, klicken Sie auf **Vorschlagen**. Es wird ein Dialogfeld mit dem neuen Passwort angezeigt, das automatisch in die Felder **Neues Passwort** und **Passwort bestätigen** eingegeben wird. Sie sollten es auf jeden Fall notieren, bevor Sie auf OK klicken und das Dialogfeld schließen.

4. Bestätigen Sie das Passwort, indem Sie es erneut in das Feld **Passwort bestätigen** eingeben.
5. Geben Sie eine **Sicherheitsfrage** und **Sicherheitsantwort** ein. Dadurch können Sie ein neues Passwort anfordern für den Fall, dass Sie Ihr Passwort vergessen.

   Hinweis: Wenn Sie auf den Link **Passwort vergessen?** auf der Anmeldeseite klicken (falls dies über die Registerkarte "System > Seitenanpassung > **Anmeldeseite** *(siehe 448)*" aktiviert wurde), wird Ihnen per E-Mail ein Link zum Ändern Ihres Passworts gesendet. Zum Ändern des Passworts müssen Sie bereits eine **Sicherheitsfrage** und **Sicherheitsantwort** festgelegt haben, und zwar über "System > **Login ändern** *(siehe 404)*".

6. Klicken Sie auf **Ändern**.

> **Hinweis:** Das Zusatzmodul für **Discovery** kann zur Verwaltung von VSA-Anmeldedaten für Benutzer und für den Portalzugriff mithilfe von **Domänenanmeldedaten** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#7293.htm)* verwendet werden.

Systemvoreinstellungen

Check-in-Richtlinie

System > Systemvoreinstellungen > Check-in-Richtlinie

Auf der Seite **Check-in-Regel** werden Gruppen-ID-Regeln definiert, die die zulässigen minimalen, maximalen und festen Werte für eine Vielzahl von Optionen steuern. Diese Richtlinien hindern Benutzer daran, Einstellungen auszuwählen, die den Windows-Servern, auf denen der Kaseya Server-Dienst ausgeführt wird, eine unnötige Last auferlegen.

Jeweils ein Feld ändern

Gehen Sie folgendermaßen vor, wenn Sie nur eine einzige Einstellung in einer Gruppe ändern müssen:

1. Geben Sie einen neuen Wert in das Feld ein, das Sie ändern möchten.
2. Lassen Sie alle anderen Felder leer. Dies deutet an, dass diese Felder unverändert bleiben.
3. Klicken Sie auf **Aktualisieren**.

Min/Max Alter für Protokolleinträge

Diese Werte bestimmen die Mindest- und Maximalwerte, die in die Optionen unter **Maximales Alter für Agent-Protokolleinträge** in "Agent > **Protokollhistorie** *(siehe 36)*" eingegeben werden können. Um einen Wert zu entfernen, geben Sie `0` (null) ein.

Check-in-Periode

Diese Werte bestimmen die Mindest- und Maximaleinstellungen, die für die **Check-in-Periode** unter "Agent > **Check-in-Kontrolle** *(siehe 68)*" eingegeben werden können. Um einen Wert zu entfernen, geben Sie `0` (null) ein.

KServer-Adresse (0 für veränderbar) – Primär/Sekundär

Es können zwei KServer-Adressfelder angegeben werden. Der Agent checkt beim primären Server ein, aber nicht beim sekundären, es sei denn, der primäre geht offline.

Wenn `0` in die Felder **Primär** oder **Sekundär** eingegeben wird und auf **Aktualisieren** geklickt wird, wird in der Spalte **KServer (1.) (2.)** der ausgewählten Gruppen-IDs `Editable` angezeigt. Benutzer können den gewünschten Namen eines Domain Name Server (DNS) oder eine beliebige IP-Adresse in die Felder **Primärer KServer** und **Sekundärer KServer** unter "Agent > **Check-in-Kontrolle**" eingeben.

Wenn diese Kontrollkästchen aktiviert sind und Sie *DNS-Namen oder IP-Adressen in diese Felder eingeben* und dann auf **Aktualisieren** klicken, zeigt die Spalte **KServer** von ausgewählten Gruppen-IDs feste DNS-Namen oder IP-Adressen an. Benutzer müssen die festen IP-Adressen in den Feldern **Primärer KServer** und **Sekundärer KServer** unter "Agent > **Check-in-Kontrolle**" verwenden.

> **Best Practices:** Obwohl eine öffentliche IP-Adresse verwendet werden kann, empfiehlt Kaseya die Verwendung eines **Domain Name Server (DNS)**-Namens für Kaseya Server. Dies wird als Vorsichtsmaßnahme empfohlen, falls die IP-Adresse geändert werden muss. Es ist einfacher, den DNS-Eintrag zu ändern, als verwaiste Agents umzuleiten.

Automatische Kontoerstellung für ausgewählte Gruppen-ID zulassen

Wenn dies aktiviert ist, werden automatisch neue Rechner-ID-Konten für ausgewählte Gruppen-IDs erstellt, wenn der Agent des Rechners das erste Mal unter Verwendung eines neuen Rechner-ID-Namens und ausgewählter Gruppen-ID beim Kaseya Server eincheckt.

Beispiel: Auf einem neuen Rechner wird ein Agent installiert. Die Gruppen-ID `acme` ist bereits vorhanden, aber die Rechner-ID `ksmith` existiert nicht. Wenn diese Option für die Gruppen-ID `acme` aktiviert ist, wird das Rechner-ID.Gruppen-ID-Konto `ksmith.acme` beim ersten Einchecken des Agent

erstellt.

> **Hinweis: Automatische Kontoerstellung für ausgewählte Gruppen-ID zulassen** ist standardmäßig ausgewählt.

So aktivieren Sie die automatische Kontoerstellung für ausgewählte Gruppen-IDs:

1. Aktivieren Sie **Automatische Kontoerstellung für ausgewählte Gruppen-ID zulassen**.
2. Wählen Sie die Gruppen-IDs im Seitenbereich aus.
3. Klicken Sie auf **Aktualisieren**.

   `Auto Enabled` wird in der Spalte **Gruppen-IDs/Auto-Kto** der ausgewählten Gruppen-IDs angezeigt.

Automatische Kontoerstellung für Gruppen ohne Regel zulassen

Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt. Wenn dies aktiviert ist, werden automatisch neue Rechner-ID-Konten für Gruppen-IDs ohne definierte **Check-in-Richtlinie** oder für Agents mit einer noch nicht vorhandenen Gruppen-ID erstellt, wenn der Agent des Rechners das erste Mal unter Verwendung eines neuen Rechner-ID-Namens beim Kaseya Server eincheckt.

> **Hinweis: Automatische Kontoerstellung für Gruppen ohne Regel zulassen** ist standardmäßig ausgewählt.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um Regelparameter auf ausgewählte Gruppen-IDs anzuwenden.

Entfernen

Klicken Sie auf **Entfernen**, um Regelparameter von ausgewählten Gruppen-IDs zu entfernen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Gruppen-IDs

Listet Rechnergruppen auf. Alle Rechner-IDs sind mit einer Gruppen-ID und optional einer Untergruppen-ID verknüpft.

Auto Kto

`Auto Enabled` bedeutet, dass die automatische Kontoerstellung für diese Gruppen-ID aktiviert wurde.

Protokollalter (Min)/Protokollalter (Max)

Listet die Einstellungen für jede Gruppen-ID auf, die in die Felder **Max Alter für Protokolleinträge einstellen** in der Kopfzeile eingegeben wurden.

KServer (1.) (2.)

Listet die zulässigen IP-Adressen/Hostnamen des primären (1.) und sekundären (2.) Servers für Gruppen-IDs auf.

Einchecken (Min)/Einchecken (Max)

Listet die Einstellungen für jede Gruppen-ID auf, die in die Felder **Check-in-Periode** in der Kopfzeile eingegeben wurden.

Benennungsrichtlinie

System > Systemvoreinstellungen > Benennungsrichtlinie

Auf der Seite **Benennungsregel** werden die IP-Adresskriterien definiert, anhand derer Rechner automatisch einer anderen Rechnergruppe zugewiesen werden. Jeder Rechnergruppe können

mehrere Benennungsregeln zugewiesen werden.

Benennungsregeln können auch das Umbenennen einer Rechner-ID erzwingen, wenn der Rechner-ID-Name nicht mit dem Computernamen übereinstimmt. Auf diese Weise kann beim Verwalten der verwalteten Rechner weniger Verwirrung entstehen.

Das Zuweisen von Rechnern zu Rechnergruppen nach IP-Adressen hat die folgenden Vorteile:

- Normalerweise stellt eine Organisation ein einzelnes Kundenunternehmen dar und Gruppen-IDs und Untergruppen stellen Standorte in diesem Unternehmen dar. Wenn ein Mitarbeiter an einen neuen Standort versetzt wird, kann der verwaltete Rechner automatisch der entsprechenden Rechnergruppe oder Untergruppe für diesen Standort neu zugewiesen werden, wenn der Agent auf dem verwalteten Rechner aus dem Netzwerk des neuen Standorts eincheckt.
- Mithilfe von **verwalteten Variablen** *(siehe 123)* können verwaltete Rechner Verfahren ausführen, die je nach der Gruppen-ID oder Untergruppen-ID auf *lokal verfügbare Ressourcen* zugreifen. Diese nützliche Funktion kann unter Verwendung von **Benennungsregel** automatisch nach IP-Adresse angewendet werden. Dies gilt selbst für höchst mobile Mitarbeiter, die zwischen verschiedenen Unternehmensstandorten reisen.
- Die Pflege mehrerer Agent-Installationspakete in Agent > **Agents bereitstellen** *(siehe 40)*, einer für jede Organisation, kann sehr viel Zeit in Anspruch nehmen. Deshalb verwenden manche Serveranbieter ein einziges Agent-Paket für die `unnamed` Organisation und führen alle Installationen mithilfe dieses Pakets aus. System > **Benennungsrichtlinie** *(siehe 406)* kann der korrekten Organisations-Gruppen-ID automatisch neue Agents – und zwar beim ersten Check-in der Agents- auf Basis von IP oder Connection-Gateway jedes verwalteten Rechners zuweisen. Agent > **Einstellungen kopieren** *(siehe 62)* kann zu einem späteren Zeitpunkt geplant werden, um bestimmte Agent-Einstellungen nach **Rechner-ID-Vorlage** *(siehe 627)* auf den Rechnertyp zu kopieren, der von der Anfangsprüfung ermittelt wurde.

Verbindungs-Gateway

Aktivieren Sie optional das Kontrollkästchen **Connection Gateway** und geben Sie die IP-Adresse des Connection Gateway ein. Der Connection Gateway ist normalerweise die WAN-Adresse des verwalteten Rechners. Diese Regel kann unabhängig auf eine Gruppen-ID angewendet werden. Der verwaltete Rechner muss diese IP-Adresse als Connection Gateway haben, um automatisch der Gruppen-ID zugewiesen zu werden.

IP-Bereich

Aktivieren Sie optional das Kontrollkästchen **IP-Bereich** und geben Sie einen IP-Adressenbereich ein, beispielsweise `192.168.1.2` – `192.168.1.254`. Diese Regel kann unabhängig auf eine Gruppen-ID angewendet werden. Die IP-Adresse des verwalteten Rechners muss in diesem Bereich liegen, um automatisch der Gruppen-ID zugewiesen zu werden.

Zwingen Sie die Rechner-ID, immer den Computernamen anzunehmen

Aktivieren Sie optional das Kontrollkästchen **Rechner-ID zwingen, immer den Computernamen anzunehmen**, um zu erzwingen, dass jeder Rechner-ID-Name mit seinem entsprechenden Computernamen übereinstimmt. Diese Regel kann unabhängig auf eine Gruppen-ID angewendet werden.

> **Hinweis:** Rechner werden bei ihrem nächsten **vollen Check-in** *(siehe 616)* in die neue Gruppen-ID umbenannt. Der **schnelle Check-in** *(siehe 616)*-Zyklus löst keine Umbenennung aus. Um eine Rechnergruppe schnell über **Benennungsrichtlinie** umzubenennen, planen Sie das Beispiel-Agent-Verfahren `Force Check-in` unter "Agent-Verfahren > **Planen/Erstellen** *(siehe 92)*".

Aktualisieren

Klicken Sie auf **Aktualisieren**, um die Benennungsregel auf die ausgewählte Rechnergruppe anzuwenden. Das System beginnt sofort, die neue Regel der Gruppen-ID beim Einchecken der Rechner beim Kaseya Server zu erzwingen.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um eine neue Benennungsregel zu vorhandenen Benennungsregeln für eine ausgewählte Rechnergruppe hinzuzufügen.

> **Hinweis:** Jeder Rechnergruppe können mehrere Benennungsrichtlinien zugewiesen werden. Verwenden Sie diese Funktion, um automatisch Rechner mit verschiedenen IP-Adressbereichen zur selben Rechnergruppe zuzuweisen.

Löschen

Klicken Sie auf **Löschen**, um die Benennungsregel aus einer Rechnergruppe zu löschen. Das System hört sofort damit auf, die Regel für die Rechnergruppe anzuwenden.

Rechnergruppe

Diese Spalte listet die für das System definierten Rechnergruppen auf. Wählen Sie das Optionsfeld neben einer **Rechnergruppe** aus, bevor Sie eine Benennungsregel aktualisieren, hinzufügen oder löschen.

Verbindungs-Gateway

Zeigt den der Rechnergruppe zugewiesenen Connection Gateway an.

IP-Bereich

Zeigt die der Rechnergruppe zugewiesenen IP-Bereiche an.

Rechner-ID erzwingen

Zeigt ein Häkchen an, wenn **Rechner-ID zwingen, immer den Computernamen anzunehmen** für eine Rechnergruppe aktiviert ist.

Benutzersicherheit

System > Benutzersicherheit

Benutzersicherheit legt den Zugriff fest, den Benutzer auf Funktionen und Datenobjekte im VSA haben. Sie werden die Konfiguration der **Benutzersicherheit** am leichtesten verstehen, wenn Sie jedes der folgenden Konzepte in der vorgelegten Reihenfolge erwägen.

1. **Scope-Datenobjekte** (siehe 423) – **Datenobjekte** sind Objekte, die von Ihnen erstellt und benannt werden. **Scope-Datenobjekte** sind wichtig, sodass sie systemweit gesichert werden müssen. Umfangsdatenobjekte umfassen Organisationen, Rechnergruppen, Rechner, Abteilungen und Service-Desks. Scope-Datenobjekte müssen *vor* der Zuweisung zu Scopes definiert werden.
2. **Scopes** (siehe 419) – Gruppen von Datenobjekten, die für Benutzer im VSA *sichtbar* sind
3. **Benutzerrollen** (siehe 414) – Sätze von VSA-Funktionen, die VSA-Benutzer ausführen dürfen. *Eine* **Funktion** *wird auf Datenobjekte angewendet.* Beispiele für Funktionen sind Öffnen, Hinzufügen, Bearbeiten oder Löschen von Datensätzen.
4. **Benutzerrollentypen** (siehe 416) – Integrierte Klassifikationen, die die Typen der *benutzerrollenbasierten* Lizenzen festlegen, die auf Benutzer in Benutzerrollen angewendet werden
5. **Rechnerrollen** (siehe 417) – Gruppen von Funktionen für den **Portalzugriff** *(siehe 75)*, die Rechnerbenutzer ausführen dürfen, wenn die VSA-Seite **Portalzugriff** auf ihrem Rechner angezeigt wird
6. **Rechnerrollentypen** (siehe 419) – Integrierte Klassifikationen, die die Typen der *rechnerrollenbasierten* Lizenzen festlegen, die auf Rechner in einer Rechnerrolle angewendet werden

7. **Benutzer** (siehe 409) – Bezieht sich auf VSA-Benutzer. Benutzer von Rechnern mit installierten Agents werden immer als *Rechnerbenutzer* bezeichnet, um sie von VSA-Benutzern zu unterscheiden.

Benutzer

System > Benutzersicherheit > Benutzer

Auf der Seite **Benutzer** werden Benutzerkonten erstellt und gelöscht. Außerdem können beim Erstellen des Benutzerkontos Benutzer zu **Rollen** *(siehe 414)* und **Scopes** *(siehe 419)* zugewiesen werden.

Jedem Benutzer müssen zumindest eine Rolle und ein Umfang zugewiesen werden. Sie können einem Benutzer zwar mehrere Rollen und Umfänge zuweisen, aber *es sind jeweils nur eine Rolle und ein Umfang gleichzeitig aktiv*. Die aktive Rolle und der aktive Umfang werden aus den Dropdown-Listen **Rolle** und **Umfang** in der oberen rechten Ecke der Seite ausgewählt. Sie können das Benutzerpasswort zurücksetzen, Benutzeranmeldungen aktivieren/deaktivieren und Benutzer abmelden, wenn Sie Zugriff auf diese Funktionen haben.

Hinweis: Benutzer können ihre eigenen Anmeldenamen, Passwörter und E-Mail-Adressen unter "System > **Voreinstellungen** *(siehe 402)*" ändern.

Warnung: Geben Sie jedem Benutzer einen eigenen eindeutigen Anmeldenamen, um die Verwaltung und das Audit Ihres VSA zu vereinfachen. Vermeiden Sie generische Anmeldenamen wie `User` oder `Admin`. Generische Anmeldenamen erschweren die Prüfung der Verwaltungsaktionen, die von jedem Benutzer unternommen werden.

Neuen Benutzer erstellen

1. Klicken Sie auf **Neu**. Das Dialogfeld **Benutzer hinzufügen** wird angezeigt.
2. Geben Sie die **Benutzerdaten** ein:
   - Geben Sie eine **E-Mail-Adresse** für den neuen Benutzer ein.
   - Wählen Sie eine **Anfangsrolle** für den neuen Benutzer aus.
   - Wählen Sie einen **Anfangsumfang** für den neuen Benutzer aus.
   - Geben Sie einen **Vornamen** und einen **Nachnamen** ein.
3. Optional können Sie auch die Daten für **Zugehöriger Org.-Mitarbeiter** eingeben:
   - Wählen Sie eine **Mitarbeiter-Org.**
   - Wählen Sie eine **Mitarbeiter-Abtlg.**
   - Geben Sie einen **Mitarbeiter** ein oder wählen Sie ihn aus.
4. Legen Sie die **Benutzer-Anmeldedaten** fest:
   - Geben Sie einen **Benutzernamen** ein.
   - Geben Sie ein Passwort in die Felder **Passwort** und **Passwort bestätigen** ein. Bei Passwörtern muss die Groß-/Kleinschreibung beachtet werden.

     Hinweis: Wenn Sie möchten, dass das System ein starkes Passwort für Sie erzeugt, klicken Sie auf **Vorschlagen**. Das neue Passwort wird automatisch in die Felder **Passwort** und **Passwort bestätigen** eingegeben. Sie sollten es auf jeden Fall notieren, bevor Sie auf OK klicken und das Dialogfeld schließen.

   - Aktivieren Sie das Kontrollkästchen **Erfordert Passwortänderung bei der nächsten Anmeldung**, damit der Benutzer bei seiner ersten Anmeldung zur Eingabe eines neuen Passworts gezwungen wird.

5. Klicken Sie auf **Speichern**. Der neue Benutzer wird im mittleren Feld angezeigt.

Vorhandenen Benutzerdatensatz ändern

1. Klicken Sie auf einen **Benutzer**, der im mittleren Feld angezeigt wird.
2. **Bearbeiten** Sie optional die folgenden Attribute des Benutzerdatensatzes:
   - **Vorname**
   - **Nachname**
   - **E-Mail-Adresse**
   - **Mitarbeiter-Org.**
   - **Mitarbeiter-Abtlg.**
   - **Mitarbeiter**
3. Fügen Sie optional Rollen über die Registerkarte **Rollen** hinzu oder entfernen Sie sie.
4. Fügen Sie optional Umfänge über die Registerkarte **Umfänge** hinzu oder entfernen Sie sie.
5. Optional können Sie auch den Zugang zu Rechnern und andere Assets auf der Registerkarte Persönlicher Scope festlegen.
6. Ändern Sie optional das Passwort, indem Sie auf die Schaltfläche **Passwort einrichten** klicken.
7. Zwingen Sie optional einen Benutzer zu einer Änderung seines Passworts, indem Sie auf die Schaltfläche **Passwort erzwingen** klicken.
8. Aktivieren/Deaktivieren Sie optional Benutzeranmeldungen, indem Sie auf die Schaltflächen **Aktivieren** oder **Deaktivieren** klicken.

Passwort einrichten

Wählen Sie im mittleren Feld einen Benutzer aus und klicken Sie auf **Passwort einrichten**, um das Passwort für den ausgewählten Benutzer zu ändern. Bei Passwörtern muss die Groß-/Kleinschreibung beachtet werden.

Passwort erzwingen

Setzt durch, dass ein ausgewählter Benutzer im mittleren Feld seinen Anmeldename bei der nächsten Anmeldung ändern muss.

Aktivieren/Deaktivieren

Wählen Sie im mittleren Feld einen Benutzer aus und klicken Sie auf **Aktivieren** oder **Deaktivieren**, um zu bestimmen, ob er sich beim VSA anmelden darf oder nicht. Dies wirkt sich nicht auf Benutzer aus, die bereits beim VSA angemeldet sind. Die Spalte **Deaktiviert** im mittleren Feld zeigt an, ob ein Benutzer an der Anmeldung am VSA gehindert wird.

Ausloggen

Eine Spalte im mittleren Feld deutet an, ob gegenwärtig ein Benutzer angemeldet ist. Wählen Sie im mittleren Feld einen anderen angemeldeten Benutzer als Sie aus und klicken Sie auf **Abmelden**, um diesen Benutzer abzumelden. *Benutzer sind immer noch angemeldet, wenn sie ihren Browser ohne Abmeldung schließen.* Die Einstellung **Leerlaufzeiten vor Ablauf einer Benutzersitzung in Minuten** unter "System > **Anmelderichtlinie** *(siehe 444)*" bestimmt, wann inaktive Benutzersitzungen automatisch abgemeldet werden.

> **Hinweis:** Eine Zusammenfassung der Funktionen, die sich auf Benutzeranmeldungen auswirken, finden Sie unter **Anmelderichtlinien für VSA** *(siehe 401)*.

Master-Benutzer vs. Standardbenutzer

Ein Master-Benutzer ist ein VSA-**Benutzer** *(siehe 616)* mit `Master`-Benutzerrolle und `Master`-Scope. Die `Master`-Benutzerrolle bietet Benutzerzugriff auf alle Funktionen im gesamten VSA. Der `Master`-Scope

stellt Zugriff auf alle Scope-Datenobjekte im gesamten VSA bereit. Eine `Master`-Benutzerrolle kann zwar mit einem Nicht-`Master`-Scope verwendet werden, ein `Master`-Scope aber nicht mit einer Nicht-`Master`-Rolle. Die Kaseya Server-Verwaltungskonfiguration und andere **spezialisierte Funktionen** *(siehe 414)* können nur von Benutzern mit `Master`-Rolle ausgeführt werden. Der Begriff *Standardbenutzer* wird manchmal für einen Benutzer ohne `Master`-Rolle und `Master`-Scope verwendet.

Master-Benutzer

- Wenn genügend Rollentyplizenzen vorhanden sind, können jedem Benutzer eine `Master`-Benutzerrolle und ein `Master`-Scope zugewiesen werden.
- Benutzer mit `Master`-*Rolle* können alle Navigations- und Kontrolloptionen anzeigen und verwenden, die in der Benutzeroberfläche zur Verfügung stehen.
- `Master`-*Scope-Benutzer* können alle Scope-Datenobjekte anzeigen, hinzufügen, bearbeiten oder löschen: Organisationen, Rechnergruppen, Rechner, Abteilungen und Service-Desks.
- Master-Benutzer können jeden Benutzer, einschließlich anderer Master-Benutzer, hinzufügen oder löschen. Da selbst ein Master-Benutzer sein eigenes Konto nicht löschen kann, während er angemeldet ist, erfordert das System, dass stets mindestens ein Master-Benutzer definiert ist.

Standardbenutzer

- Ein Standard-Rollenbenutzer kann keine Rollen sehen, für die ihm keine Anzeigeberechtigung gewährt wurde.
- Ein Standard-Umfangbenutzer kann keine Datenobjekte oder Benutzer sehen, für die ihm keine Anzeigeberechtigung gewährt wurde.
- Standardbenutzer können andere Benutzer, Umfänge und Rollen erstellen, wenn ihnen der Zugriff auf diese Funktionen gewährt wurde.
- Ein Standardbenutzer kann *keine* weiteren Zugriffsberechtigungen zu denjenigen gewähren, über die der Standardbenutzer verfügt.
- Wenn Standardbenutzern der Funktionszugriff erteilt wird, können sie nur andere Standardbenutzer (keine Master-Benutzer) erstellen.
- Standardmäßig übernimmt ein neuer Standardbenutzer die Umfänge und Rollen des Standardbenutzers, der ihn erstellte.
- Wenn ein Master-Benutzer einen neuen Standardbenutzer erstellt, übernimmt der Standardbenutzer *keine* Umfänge oder Rollen. Bei Verwendung dieser Methode muss der Master-Benutzer die Umfänge und Rollen des neuen Standardbenutzers manuell zuweisen.

Rechnerbenutzer

- Rechnerbenutzer verwenden Rechner, auf denen VSA-Agents installiert sind. Sie dürfen nicht mit VSA-Benutzern verwechselt werden, die sich beim VSA anmelden können.
- Rechnerbenutzer können auf das Agent-Symbol in der Systemablage des Rechners klicken, um das VSA-Fenster **Portalzugriff** *(siehe 75)* mit Funktionen und Daten nur für diesen Rechner anzuzeigen. Der **Portalzugriff** wird als **Live-Connect** *(siehe 393)* bezeichnet, wenn der Zugriff über den VSA erfolgt.
- Der Zugriff auf **Portalzugriffs**-Funktionen wird von der Rechnerrolle bestimmt, der der Rechner zugewiesen ist. Verwaltete Rechner werden standardmäßig der Rechnerrolle `Default` zugewiesen und haben Zugriff auf alle **Portalzugriff**-Funktionen, vorausgesetzt, sie wurden nicht von einem VSA-Benutzer eingeschränkt.
- Der Datenobjektzugriff über den Rechner wird vom **Scope** *(siehe 419)* `Anonymous` bestimmt. Gegenwärtig sind die einzigen vom Scope `Anonymous`aktivierten Datenobjekte **Service Desk**-Tickets. Alle anderen in **Portalzugriff** angezeigten Daten werden vom Rechner selbst erzeugt.

Neuen Master-Benutzer erstellen

Benutzerpasswort vergessen

Sollten Sie das Passwort für Ihr Master-Benutzerkonto vergessen haben, kann das System ein neues Master-Benutzerkonto für Sie erstellen oder das Passwort eines bestehenden Master-Benutzerkontos zurücksetzen. Damit können Sie sich wieder beim System anmelden und die vergessenen Kontoinformationen abrufen. Ein Master-Benutzer ist ein VSA-**Benutzer** *(siehe 616)* mit `Master`-Benutzerrolle und `Master`-Scope.

> **Hinweis:** Sie müssen über Administratorberechtigungen auf dem Kaseya Server verfügen. Aus Sicherheitsgründen können Sie das folgende Verfahren nicht remote ausführen.

Neues Master-Benutzerkonto erstellen

1. Melden Sie sich auf dem Rechner an, auf dem der Kaseya Server ausgeführt wird.
2. Rufen Sie diese Webseite auf: `http://localhost/LocalAuth/setAccount.asp`.
3. Geben Sie einen neuen Kontonamen in das Feld **Master-Benutzername** ein.
4. Geben Sie ein Passwort in das Feld **Passwort eingeben** ein und bestätigen Sie es, indem Sie es erneut in das Feld **Passwort bestätigen** eingeben.
5. Geben Sie im Feld **E-Mail-Adresse** eine E-Mail-Adresse ein.
6. Klicken Sie auf **Erstellen**.

Jetzt können Sie sich über das neue Master-Benutzerkonto beim System anmelden.

Passwort eines bestehenden Master-Benutzers zurücksetzen

> **Hinweis:** Das Master-Benutzerkonto kann nicht deaktiviert werden.

1. Melden Sie sich auf dem Rechner an, auf dem der Kaseya Server ausgeführt wird.
2. Rufen Sie diese Webseite auf: `http://localhost/LocalAuth/setAccount.asp`.
3. Geben Sie den Namen eines bestehenden aktiven Master-Benutzerkontos in das Feld **Master-Benutzername** ein.
4. Geben Sie ein Passwort in das Feld **Passwort eingeben** ein und bestätigen Sie es, indem Sie es erneut in das Feld **Passwort bestätigen** eingeben.
5. Überspringen Sie die **E-Mail-Adresse**. Auf dieser Webseite kann die E-Mail-Adresse eines bestehenden Benutzers nicht zurückgesetzt werden.
6. Klicken Sie auf **Erstellen**.

Jetzt können Sie sich über das bestehende Master-Benutzerkonto wieder beim System anmelden.

Wenn Ihr Konto deaktiviert wurde

Für den Fall, dass Ihr VSA-Konto deaktiviert wurde, weil Sie zu oft ein falsches Passwort eingegeben haben, können Sie festlegen, dass das Konto nach Ablauf eines gewissen Zeitraums automatisch wieder aktiviert wird. Dieser Zeitraum beträgt standardmäßig 1 Stunde, kann aber von Ihrem VSA-Systemadministrator geändert werden.

Sollte Ihr Konto aus einem anderen Grund deaktiviert worden sein, wenden Sie sich an Ihren VSA-Systemadministrator, um es wieder zu aktivieren. Durch Zurücksetzen des Passworts können deaktivierte Benutzerkonten nicht wieder aktiviert werden.

Informationen zum Erstellen eines neuen Hauptkontos auf dem Kaseya Server finden Sie unter: **Neuen Master-Benutzer erstellen** *(siehe 412)*

Passwörter externer Anwendungen ändern

Externe Anwendungen und Authentifizierung mit der Web-Service-API

Externe Anwendungen können über die **Web-Service-API** *(siehe 532)* in den VSA integriert werden. Diese externen Anwendungen können von unabhängigen Softwareanbietern wie Autotask, ConnectWise oder Tigerpaw oder auch von Beratungsfirmen oder anderen Unternehmen mit spezifischem technischen Fachwissen entwickelt werden. Zur Nutzung der Web-Service-API müssen externe Anwendungen so programmiert sein, dass sie über einen gültigen Satz von VSA-Benutzername und -Passwort authentifiziert werden können.

Änderungen an Passwörtern in V6.2 mit Auswirkung auf externe Anwendungen

Bis zu VSA v6.1 wurde zum Hashen von Passwörtern ein SHA-1-Algorrithmus eingesetzt. Daher kamen in mit v6.1 kompatiblen Anwendungen auch SHA-1-basierte Authentifizierungsmethoden zum Einsatz. Ab v6.2 werden in v6.2 erstellte Passwörter mit einem SHA-256-Algorithmus gehasht. In früheren VSA-Versionen erstellte Passwörter bleiben so lange mit SHA-1 gehasht, bis das Passwort geändert oder der Benutzer umbenannt wird. Dann kommt auch für diese Passwörter SHA-256 zum Einsatz. Externe Anwendungen, die in v6.1 genutzt wurden, müssen über eine Änderung der Programmierung dahingehend aktualisiert werden, dass sie die SHA-256-Passwörter aus v6.2 unterstützen.

Externe Anwendungen und Passwörter aktualisieren

Wenn Sie Version v6.1 oder früher des VSA mit einer externen Anwendung genutzt haben, müssen Sie für die Kompatibilität der verwendeten Anmeldedaten sorgen. Kaseya empfiehlt, die externe Anwendung auf eine mit VSA v6.2 kompatible Version zu aktualisieren. Bis dahin können Sie mithilfe des unter **Neue SHA-1-Anmeldedaten für externe Legacy-Anwendungen erstellen** beschriebenen Vorgangs für Kompatibilität mit Programmen für Drittanbietern sorgen.

> **Warnung:** Jegliche Änderung des Passworts einer externen Legacy-Anwendung führt zu einer **Unterbrechung der Integration**, bis entweder die externe Anwendung zur Nutzung des erforderlichen SHA-256-Hash-Algorithmus aktualisiert wurde oder neue SHA-1-Anmeldedaten erstellt und angewendet wurden. Stellen Sie also sicher, dass keine Passwörter externer Anwendungen geändert werden, bevor die Aktualisierung vorgenommen wurde.

Wenn Sie in VSA v6.1 oder früher mit einer externen Anwendung eines unabhängigen Softwareanbieters oder anderen Herstellers gearbeitet haben:

1. Wenden Sie sich an den Hersteller der externen Anwendung.
2. Fordern Sie eine aktualisierte Version an.
3. Implementieren Sie die aktualisierte Version.
4. Wenn dies erfolgt ist, können Sie das Passwort ändern oder das Benutzerkonto umbenennen, die von der externen Anwendung genutzt werden.

Informationen für unabhängige Softwareanbieter oder andere Entwickler externer Anwendungen

1. Gehen Sie in der Online-Hilfe zum Abschnitt **Hash-Algorithmus** im Thema **Authentifizierung** *(siehe 547)* . Hier finden Sie Anleitungen zur Aktualisierung der externen Anwendung, um die gleichzeitige Kompatibilität mit VSA v6.2 und früheren Versionen des VSA zu gewährleisten.
2. Implementieren Sie die erforderlichen Programmmierungsänderungen in der externen Anwendung.

Neue SHA-1-Anmeldedaten für externe Legacy-Anwendungen erstellen

Wenn Sie in VSA v6.2 oder höher einen kompatiblen Satz aus SHA-1-Benutzernamen und -Passwort für eine externe Legacy-Anwendung anlegen müssen, die noch nicht auf Kompatibilität mit v6.2-Passwörtern aufgerüstet wurde, gehen Sie wie folgt vor: Erstellen Sie entweder einen neuen Master-Benutzer mit zugehörigem Passwort oder setzen Sie das Passwort des bestehenden Master-Benutzers zurück.

> **Hinweis:** Sie müssen über Administratorberechtigungen auf dem Kaseya Server verfügen. Aus Sicherheitsgründen können Sie das folgende Verfahren nicht remote ausführen.

Neues Master-Benutzerkonto erstellen

1. Melden Sie sich auf dem Rechner an, auf dem der Kaseya Server ausgeführt wird.
2. Rufen Sie diese Webseite auf: `http://localhost/localAuth/setAccountV61.asp`.
3. Geben Sie einen neuen Kontonamen in das Feld **Master-Benutzername** ein.
4. Geben Sie ein Passwort in das Feld **Passwort eingeben** ein und bestätigen Sie es, indem Sie es erneut in das Feld **Passwort bestätigen** eingeben.
5. Geben Sie im Feld **E-Mail-Adresse** eine E-Mail-Adresse ein.
6. Klicken Sie auf **Erstellen**.

Die externe Anwendung kann nun aktualisiert werden, um sich über das neue Benutzerkonto und SHA-1-Passwort mit dem VSA zu verbinden.

Passwort eines bestehenden Master-Benutzers zurücksetzen

> **Hinweis:** Das Master-Benutzerkonto kann nicht deaktiviert werden.

1. Melden Sie sich auf dem Rechner an, auf dem der Kaseya Server ausgeführt wird.
2. Rufen Sie diese Webseite auf: `http://localhost/localAuth/setAccountV61.asp`.
3. Geben Sie den Namen eines bestehenden aktiven Master-Benutzerkontos in das Feld **Master-Benutzername** ein.
4. Geben Sie ein Passwort in das Feld **Passwort eingeben** ein und bestätigen Sie es, indem Sie es erneut in das Feld **Passwort bestätigen** eingeben.
5. Überspringen Sie die **E-Mail-Adresse**. Auf dieser Webseite kann die E-Mail-Adresse eines bestehenden Benutzers nicht zurückgesetzt werden.
6. Klicken Sie auf **Erstellen**.

Die externe Anwendung kann nun aktualisiert werden, um sich über das neue SHA-1-Passwort mit dem VSA zu verbinden.

Benutzerrollen

System > Benutzersicherheit > Benutzerrollen

Auf der Seite **Benutzerrollen** (siehe 414) werden Benutzerrollen erstellt und gelöscht. Innerhalb einer Rolle können Sie Folgendes auswählen:

- **Mitglieder** *(siehe 415)* – Weisen Sie einer Benutzerrolle Mitglieder zu bzw. entfernen Sie sie.
- **Zugriffsrechte** *(siehe 415)* – Wählen Sie die Zugriffsrechte für die Benutzerrolle aus. Zugriffsrechte bestimmen die Funktionen, auf die ein *Benutzer* Zugriff hat.
- **Rollentypen** *(siehe 416)* – Weisen Sie einer Benutzerrolle Rollentypen zu bzw. entfernen Sie sie. Zugriffsrechte werden von einem Satz von lizenzierten Rollentypen beschränkt, die der betreffenden Benutzerrolle zugewiesen sind.

VSA-Benutzer können zu einer oder mehreren VSA-Benutzerrolle(n) gehören. Jeder Benutzerrolle muss zumindest ein Benutzerrollentyp zugewiesen werden.

> **Hinweis:** Ein VSA-Benutzer meldet sich mit einer Benutzerrolle (die Funktionen, die er ausführen kann) und einem Scope (die Scope-Datenobjekte, die er sehen kann) an. Die Mitgliedschaft in einer Benutzerrolle und die Mitgliedschaft in einem Umfang sind voneinander unabhängig.

Hinweis: Auf der Registerkarte "System > **Benutzer** *(siehe 409)* > Rollen" können VSA-Benutzer auch Benutzerrollen zugewiesen werden.

Hinweis: Eine Erläuterung der `Master`-Benutzerrolle finden Sie unter "System > **Benutzer** *(siehe 409)*".

Warnung: Beschränken Sie den Zugriff auf **Benutzerrollen** und **Rechnerrollen** für alle Rollen außer die, die für den Zugriff auf Verwaltungsfunktionen verantwortlich sind.

Mittleres Feld

Im mittleren Feld von **Rollen** können Sie Folgendes ausführen:

- **Neu** – Erstellen Sie eine neue Rolle.
- **Berechtigungen kopieren** – Kopieren Sie die Zugriffsrechte für die ausgewählte Rolle aus einer anderen Rolle.
- **Umbenennen** – Benennen Sie die Rolle um. Rollennamen können nur in Kleinbuchstaben eingegeben werden.
- **Löschen** – Löschen Sie die ausgewählte Rolle. Alle VSA-Benutzer müssen aus einer Rolle entfernt werden, bevor sie gelöscht werden kann.

Verwandte Seiten

Die folgenden Regeln werden nach Benutzerrolle zugewiesen:

- Zugriff auf den gesamten VSA nach Wochentag und Stunde über "System > **Anmeldestunden** *(siehe 422)*"
- Remote-Control-Benutzerbenachrichtigung über "Remote Control > **Benutzerrollen-Richtlinie** *(siehe 382)*"
- Feldberechtigungen zum Bearbeiten von Tickets in "Ticketing > **Felder bearbeiten** *(siehe 471)*" und "Service-Desk > Rollenvoreinstellungen"
- **Gemeinsam nutzbare Objekte** *(siehe 421)* (z. B. Verfahren, Berichte, Monitor-Sets und Agent-Installationspakete) können nach Benutzerrolle freigegeben werden.

Registerkarte "Mitglieder"

Auf der Registerkarte **Mitglieder** wird angezeigt, welche VSA-Benutzer der im mittleren Feld ausgewählten Rolle zugewiesen sind.

- Klicken Sie auf die Schaltflächen **Zuweisen** und **Entfernen**, um die Rolle zu ändern, der VSA-Benutzer zugewiesen sind.
- Sortieren und filtern Sie die VSA-Benutzer, die auf der Seite **Mitglieder** aufgeführt werden.

Registerkarte "Zugriffsrechte"

Auf der Registerkarte **Zugriffsrechte** der Seite "System > **Benutzerrollen**" wird festgelegt, welche Funktionen VSA-Benutzer, die zu einer ausgewählten Rolle gehören, ausführen dürfen. Zum Beispiel können Zugriffsrechte einschließen, ob ein Benutzer einen bestimmten Datensatz öffnen, hinzufügen, bearbeiten oder löschen darf.

Hinweis: Scopes bestimmen, ob ein Benutzer bestimmte benutzererstellte Datenstrukturen *sehen* kann, die im VSA angezeigt werden. **Rollen** legen die Zugriffsrechte auf die Funktionen fest, die an diesen Datenstrukturen ausgeführt werden können.

Eine Navigationsstruktur bietet Zugriff auf alle Module, Ordner, Elemente und Steuerelemente im VSA.

- Klicken Sie auf die Symbole ⊞ oder ⊟ neben einem Element in der Struktur, um untergeordnete Verzweigungen dieses Elements ein- oder auszublenden.

- Ein markiertes Element bedeutet, dass eine Rolle den Zugriff darauf bietet.
- Ein nicht markiertes Element bedeutet, dass eine Rolle *keinen* Zugriff darauf hat.
- Klicken Sie auf **Alles erweitern**, um die gesamte Struktur zu erweitern.
- Klicken Sie auf **Alles reduzieren**, um die gesamte Struktur zu reduzieren.

- Klicken Sie auf **Rollenzugriffsrechte konfigurieren**, um die Zugriffsrechte für eine Rolle zu ändern.
  - Durch Aktivieren oder Deaktivieren der Kontrollkästchen wird derselbe Status für untergeordnete Elemente eingestellt.
  - Klicken Sie auf **Alle aktivieren**, um alle Elemente zu aktivieren.
  - Klicken Sie auf **Alle deaktivieren**, um alle Elemente zu deaktivieren.

Spezielle Zugriffsrechte

- Infocenter > Dashboard > **Administratorhinweise**
- Infocenter > Dashboard > **Status**
- Infocenter > Dashboard > **Online-Hilfe**
- Schnellansicht – Wenn Sie den Cursor auf ein Check-in-Symbol bewegen, wird sofort das **Agent-Schnellansichtsfenster** geöffnet. Im **Agent-Schnellansichtsfenster** können Sie Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten. Mithilfe von **Agent-Zeichen** *(siehe 18)* können Sie Text für **besondere Anweisungen** am unteren Rand des **Schnellansichtsfensters** anzeigen.
  - **Schnellstartfunktionen** – Zeigt die Aktionsschaltflächen am oberen Rand des Schnellansicht-Popupfensters an oder blendet sie aus.
  - **Verfahren jetzt ausführen**
    - ✓ **Verfahren ausführen** – Zeigt alle Agent-Verfahren in der Liste **Verfahren ausführen** der Schnellansicht an oder blendet sie aus.
    - ✓ **Verfahrensliste bearbeiten** – Zeigt die Schaltflächen zum Hinzufügen und Löschen in der Liste **Verfahren ausführen** der Schnellansicht an oder blendet sie aus.
    - ✓ **Einstellungen ändern** – Zeigt das Zahnradsymbol für die Einstellungen in der Titelleiste der Schnellansicht an oder blendet sie aus. In den Einstellungen können Benutzer die Liste der Optionen im Schnellansicht-Popupfenster nach eigenem Ermessen anzeigen, ausblenden oder neu anordnen.
  - **Schnellansichtdaten** – Zeigt die Optionen zu den Agent-Daten im Schnellansicht-Popupfenster an oder blendet sie aus.
- System > Systemvoreinstellungen > **Funktionaler Zugriff** – *(veraltet)*
- System > Systemvoreinstellungen > **Planung aktivieren** – Gilt für die Schaltfläche **Planen** ausschließlich im Zusammenhang mit folgenden Funktionen. Mehr darüber erfahren Sie in der **Kaseya Knowledge Base** *(https://helpdesk.kaseya.com/entries/33901207)*.
  - Patch-Verwaltung > Rechner verwalten > Rechner scannen
  - Patch-Verwaltung > Rechner verwalten > Anfangsupdate
  - Patch-Verwaltung > Rechner verwalten > Automatisches Update
  - Infocenter > Berichterstellung> Berichte
  - Infocenter > Berichterstellung > Berichtssets
- System > Systemvoreinstellungen > Wake-on-LAN aktivieren – Gilt nur für die Schaltfläche "Patch-Verwaltung > Rechner scannen > Planen".

Registerkarte "Rollentypen"

Klicken Sie auf die Schaltflächen **Zuweisen** und **Entfernen**, um die Rollentypen zu ändern, denen eine Benutzerrolle zugewiesen ist.

Rollentypen

Kaseya-Lizenzen werden nach Rollentyp erworben. Es gibt separate Rollentypen zur Lizenzierung von Benutzern nach *Benutzerrollentyp* und zur Lizenzierung von Rechnern nach *Rechnerrollentyp*. Die einzelnen Rollen ermöglichen die Nutzung festgelegter Funktionen, die unter "Benutzerrollen > **Zugriffsrechte** *(siehe 415)*" bzw. "Rechnerrollen > **Zugriffsrechte** *(siehe 418)*" aufgelistet sind. Die Anzahl der erworbenen Rollentyplizenzen wird auf der Registerkarte "System > **Lizenzmanager** *(siehe 438)* > Rollentyp" angezeigt. Jede Rollentyplizenz gibt die Anzahl der zulässigen *genannten Benutzer* und *gleichzeitigen Benutzer* an.

Benutzerrollentypen

Jeder Benutzerrolle muss zumindest ein Benutzerrollentyp zugewiesen werden. Wird eine Benutzerrolle mehr als einem Rollentyp zugewiesen, wird der Zugriff auf eine Funktion aktiviert, wenn einer der Rollentypen den Zugriff auf diese Funktion zulässt. Der Funktionszugriff kann optional noch weiter nach Benutzerrolle oder Rechnerrolle eingeschränkt werden. Beispiele für Benutzerrollentypen umfassen etwa:

- **VSA-Admin** – Schließt sowohl Master-Benutzer als auch Standardbenutzer ein.
- **Endbenutzer** – Bietet eingeschränkten Zugriff auf ausgewählte Funktionen im VSA. Dies ist hauptsächlich für Kunden von Dienstanbietern gedacht. Kunden können sich beim VSA anmelden und Berichte drucken oder Tickets ihrer eigenen Organisation einsehen.
- **Service-Desk-Techniker** – Kann **Service Desk**-Tickets bearbeiten und Berichte ausführen, aber keine Service-Desks, Supporttabellen oder Service-Desk-Verfahren konfigurieren.
- **Service-Desk-Admin** – Hat Zugriff auf alle Funktionen in **Service Desk**.
- Je nach erworbenem Paket gibt es noch weitere **SaaS** *(siehe 631)*-Benutzerrollentypen.

Rechnerrollen

System > Benutzersicherheit > Rechnerrollen

Auf der Seite **Rechnerrollen** (siehe 414) werden Rechnerrollen erstellt und gelöscht. Rechnerrollen bestimmen, was *Rechnerbenutzern* bei der Verwendung des **Portalzugriffs** *(siehe 75)* – einer Version von **Live-Connect** *(siehe 393)* – auf einem Rechner mit Agent angezeigt wird. Das Fenster **Portalzugriff** wird angezeigt, wenn ein *Rechnerbenutzer auf das Agent-Symbol in der Systemablage seines verwalteten Rechners doppelklickt.*

> **Hinweis:** Die Seite **Benutzerrollen** bestimmt, was *VSA-Benutzern* bei der Verwendung von **Live-Connect** innerhalb des VSA angezeigt wird.

Auf der Seite **Rechnerrollen** können Sie Folgendes auswählen:

- **Mitglieder** *(siehe 418)* – Weisen Sie einer Rechnerrolle Rechner zu bzw. entfernen Sie sie.
- **Zugriffsrechte** *(siehe 418)* – Wählen Sie die Zugriffsrechte für die Rechnerrolle aus. Zugriffsrechte bestimmen die Funktionen, auf die ein *Rechnerbenutzer* Zugriff hat.
- **Rollentypen** *(siehe 419)* – Weisen Sie einer Rechnerrolle Rollentypen zu bzw. entfernen Sie sie. Gegenwärtig gibt es nur einen Rechnerrollentyp. Eine Beschränkung der Zugriffsrechte findet nicht statt.

> **Hinweis:** Die **Startseite**, die Rechnerbenutzer beim erstmaligen Öffnen des Fensters **Portalzugriff** sehen, kann über "System > Anpassen > **Live-Connect** *(siehe 452)* festgelegt werden.
>
> **Hinweis:** Siehe **Ticketing für Portalzugriffbenutzer auf nicht unterstützten Browsern aktivieren** *(siehe 76)*.
>
> **Hinweis:** Weitere Hinweise finden Sie in der PDF-Schnellstartanleitung Agent Configuration and Deployment **(Konfiguration und Bereitstellung von Agents)** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/DE_RCtools70.pdf#zoom=70&navpanes=0)*.

Die Standardrechnerrolle

Bei der Installation des VSA wird eine vordefinierte `Default`-Rechnerrolle bereitgestellt. Neu erstellte Rechner-ID-Konten werden automatisch der `Default`-Rechnerrolle zugewiesen. Wenn Sie andere Rechnerrollen erstellen, können Sie ihnen Rechner-ID-Konten neu zuweisen. Dies wäre eventuell der Fall, wenn Sie den Rechnerbenutzerzugriff auf Funktionen auf der Seite **Portalzugriff** für verschiedene Gruppen von Rechnerbenutzern beschränken möchten. Jedes Rechner-ID-Konto kann nur zu einer einzigen Rechnerrolle gehören.

Mittleres Feld

Im mittleren Feld von **Rechnerrollen** können Sie Folgendes ausführen:

- **Neu** – Erstellen Sie eine neue Rechnerrolle.
- **Berechtigungen kopieren** – Kopieren Sie die Zugriffsrechte für die ausgewählte Rechnerrolle aus einer anderen Rechnerrolle.
- **Umbenennen** – Benennen Sie die Rechnerrolle um.
- **Löschen** – Löschen Sie die ausgewählte Rechnerrolle. Alle Rechner müssen aus einer Rechnerrolle entfernt werden, bevor Sie die Rolle löschen können.

Registerkarte "Mitglieder"

Auf der Registerkarte **Mitglieder** wird angezeigt, welche Rechner zur im mittleren Feld ausgewählten Rechnerrolle gehören.

- Klicken Sie auf die Schaltfläche **Rechnerrolle ändern**, um die Rechnerrolle zu ändern, der ein Rechner zugewiesen ist.
- Sortieren und filtern Sie die Rechner, die auf der Seite **Mitglieder** aufgeführt werden.

Registerkarte "Zugriffsrechte"

Auf der Registerkarte **Zugriffsrechte** der Seite "System > **Rechnerrollen**" wird festgelegt, welche Funktionen *Rechnerbenutzer*, die zu einer ausgewählten Rechnerrolle gehören, auf den Rechnern ausführen dürfen. Zum Beispiel können die Zugriffsrechte einschließen, ob ein Rechnerbenutzer remote von einem anderen Rechner auf seinen eigenen Rechner zugreifen kann.

Eine Navigationsstruktur bietet Zugriff auf jedes Element und jede Steuerung auf der Seite **Live Connect**.

- Klicken Sie auf die Symbole ⊞ oder ⊟ neben einem Element in der Struktur, um untergeordnete Verzweigungen dieses Elements ein- oder auszublenden.
  - Ein markiertes Element bedeutet, dass ein Rechner den Zugriff darauf bietet.
  - Ein nicht markiertes Element bedeutet, dass eine Rechnerrolle *keinen* Zugriff darauf hat.
  - Klicken Sie auf **Alles erweitern**, um die gesamte Struktur zu erweitern.
  - Klicken Sie auf **Alles reduzieren**, um die gesamte Struktur zu reduzieren.
- Klicken Sie auf **Rollenzugriffsrechte konfigurieren**, um die Zugriffsrechte für eine Rechnerrolle zu ändern.
  - Durch Aktivieren oder Deaktivieren der Kontrollkästchen wird derselbe Status für untergeordnete Elemente eingestellt.
  - Klicken Sie auf **Alle aktivieren**, um alle Elemente zu aktivieren.
  - Klicken Sie auf **Alle deaktivieren**, um alle Elemente zu deaktivieren.

Registerkarte "Rollentypen"

> **Hinweis:** In der vorliegenden Version von Kaseya 2 gibt es nur einen Rollentyp; das bedeutet, dass alle Rechner den Rollentyp **Basic Machine** verwenden müssen.

- **Basic Machine** – Bietet Zugriff auf alle **Portalzugriffs**funktionen, die Rechnerbenutzern zur Verfügung stehen.

Rollentypen

Kaseya-Lizenzen werden nach Rollentyp erworben. Es gibt separate Rollentypen zur Lizenzierung von Benutzern nach *Benutzerrollentyp* und zur Lizenzierung von Rechnern nach *Rechnerrollentyp*. Die einzelnen Rollen ermöglichen die Nutzung festgelegter Funktionen, die unter "Benutzerrollen > **Zugriffsrechte** *(siehe 415)*" bzw. "Rechnerrollen > **Zugriffsrechte** *(siehe 418)*" aufgelistet sind. Die Anzahl der erworbenen Rollentyplizenzen wird auf der Registerkarte "System > **Lizenzmanager** *(siehe 438)* > Rollentyp" angezeigt. Jede Rollentyplizenz gibt die Anzahl der zulässigen *genannten Benutzer* und *gleichzeitigen Benutzer* an.

Rechnerrollentypen

Jede Rechnerrolle muss einem Rechnerrollentyp zugewiesen werden. *In der Erstversion von Kaseya 2 gibt es nur einen Rechnerrollentyp.* Der Rechnerrollentyp bestimmt den Typ der *rechnerbasierten Lizenz*, die auf in einer Rechnerrolle eingeschlossene Rechner angewendet werden soll. Wenn Sie beispielsweise eine Rechnerrolle namens `StdMach` erstellen, `StdMach` dem Rechnerrollentyp namens `Basic Machine` zuweisen und es 150 Rechner in der Rechnerrolle `StdMach` gibt, dann werden unter "System > **Lizenzmanager** *(siehe 438)*" 150 der insgesamt verwendeten `Basic Machine`-Lizenzen angezeigt.

Scopes

System > Benutzersicherheit > Scopes

Auf der Seite **Scopes** (siehe 419) wird die *Sichtbarkeit* gewisser Typen von benutzerdefinierten Datenobjekten im ganzen VSA definiert. Zum Beispiel könnte ein Benutzer einige Rechnergruppen sehen, aber nicht in der Lage sein, andere Rechnergruppen zu sehen. Nachdem ein Umfang ein Datenobjekt für einen Benutzer sichtbar gemacht hat, werden die Funktionen, die der Benutzer am Datenobjekt ausführen kann, nach Benutzerrolle festgelegt. Mithilfe von Scopes können für die Benutzersicherheit zuständige VSA-Benutzer verschiedene Umfänge von Datenobjekten erstellen und unterschiedlichen Benutzergruppen zuweisen.

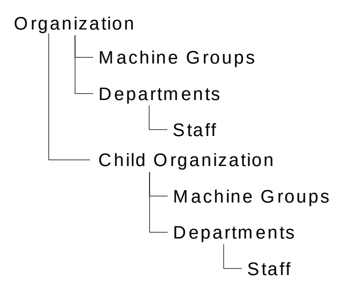
> **Hinweis:** Ein Benutzer meldet sich mit einer zugewiesenen Rolle (die Funktionen, die er ausführen kann) und einem zugewiesenen Scope (die Daten, die er sehen kann) an. Die Mitgliedschaft in einer Rolle und in einem Scope sind voneinander unabhängig.

Auf der Registerkarte "System > **Benutzer** *(siehe 409)* > Scopes" können Benutzer auch Scopes zugewiesen werden.

Umfangsdatenobjekte

Es gibt fünf Typen an Datenobjekten, die Scopes zugewiesen werden können. Jedes Datenobjekt wird außerhalb von Umfängen definiert, bevor es Umfängen zugewiesen wird.

- **Organisationen** – Organisationen sind normalerweise Kunden, aber nicht unbedingt. Ein Organisationsdatensatz enthält gewisse allgemeine Informationen, beispielsweise den Namen und die Adresse, die Anzahl der Mitarbeiter und die Website. Eine Organisation definiert außerdem eine Hierarchie an zusätzlichen Informationen (siehe unten), die die Rechnergruppen und Angestellten in dieser Organisation darstellen. Organisationen werden über "System > Orgn./Gruppen/Abtlg./Personal > **Verwalten** *(siehe 423)*" definiert.



- **Rechnergruppen** – Rechnergruppen sind Gruppen von verwalteten Rechnern innerhalb einer Organisation. Rechnergruppen werden über "System > Orgn./Gruppen/Abtlg./Personal > Verwalten> Rechnergruppen" definiert.
- **Rechner** – Ein verwalteter Rechner ist ein Computer, auf dem ein Agent installiert ist. Jeder Rechner muss zu einer Rechnergruppe gehören. Rechner werden üblicherweise auf der Seite "Agents > **Agents verteilen**" eingerichtet.
- **Abteilungen** – Eine Abteilung ist eine Gruppe von Mitarbeitern innerhalb einer Organisation. Ein Mitarbeiter ist nicht unbedingt dasselbe wie ein Rechnerbenutzer. Abteilungen und Mitarbeiter werden über "System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Abteilungen" definiert.
- **Service-Desk** – Service-Desks dienen zur Verarbeitung von Tickets mithilfe des **Service Desk**-Moduls. Service-Desks werden über "Service-Desk > Desk-Konfiguration > Desk-Definition" eingerichtet.

Umfangszuweisung

Die übergeordneten/untergeordneten Beziehungen zwischen Datenstrukturen wirken sich auf die Pflege von Umfängen aus.

Implizite Zuweisung

Bei der *impliziten* Zuweisung eines übergeordneten Datensatzes zu einem Umfang werden alle untergeordneten Datensätze demselben Umfang zugewiesen. Zum Beispiel wird beim Zuweisen einer Organisation zu einem Umfang Folgendes in denselben Umfang eingeschlossen:

- Untergeordnete Organisationen
- Rechnergruppen der Organisation und alle untergeordneten Organisationen
- Rechner der Rechnergruppen in dieser Organisation und alle untergeordneten Organisationen
- Abteilungen in der Organisation und alle untergeordneten Organisationen

Explizite Zuweisung

Eine Organisation der höchsten Ebene kann nur durch manuelles Hinzufügen in einen Umfang eingeschlossen werden, da kein übergeordneter Datensatz existiert, in den sie eingeschlossen werden kann. Dies wird als explizite Zuweisung bezeichnet. Sie können auch ein Objekt auf niedriger Ebene explizit einem Umfang zuweisen, *aber nur dann, wenn dieses Objekt nicht bereits dem Umfang über sein übergeordnetes Objekt explizit zugewiesen wurde.* Zum Beispiel können Sie eine Rechnergruppe explizit einschließen, ohne die übergeordnete Organisation der Rechnergruppe hinzuzufügen. Außerdem können Sie einzelne Rechner und Abteilungen explizit in einen Umfang einschließen, ohne ihre übergeordneten Datensätze einzuschließen.

Alle im Scope

Die Funktion **Umfänge** stellt gegebenenfalls die Schaltfläche **Alle im Umfang** bereit. Diese Schaltfläche

zeigt ein Fenster mit allen Datensätzen auf einer bestimmten Umfang-Registerkarte an. Dabei kommt es nicht darauf an, ob die Datensätze implizit oder explizit zugewiesen wurden.

Haupt-Umfang

Eine Erläuterung des `Master`-Scope finden Sie unter "System > **Benutzer** *(siehe 409)*".

Mittleres Feld

Im mittleren Feld von **Rollen** können Sie Folgendes ausführen:

- **Neu** – Erstellen Sie einen neuen Umfang.
- **Umbenennen** – Benennen Sie den Umfang um.
- **Löschen** – Löschen Sie den ausgewählten Umfang. Alle VSA-Benutzer müssen aus einem Scope entfernt werden, bevor er gelöscht werden kann.

Umfangdetails

Auf jeder Registerkarte können Sie Folgendes ausführen:

- **Zuweisen** – Weisen Sie den Zugriff auf eine Datenstruktur zu einem Umfang zu.
- **Entfernen** – Entfernen Sie den Zugriff auf eine Datenstruktur aus einem Umfang.
- **Alle im Umfang** – Dies wird nur auf den Registerkarten **Organisationen**, **Rechnergruppen**, **Rechner** und **Abteilungen** angezeigt. Wenn Sie auf die Schaltfläche **Alle im Umfang** auf einer Registerkarte klicken, wird ein neues Fenster mit einer Liste aller Datenstrukturen dieses Registerkartentyps im Umfang angezeigt, ob explizit oder implizit definiert.

Benutzerobjekte freigeben

Jeder Benutzer kann Benutzerobjekte erstellen, z. B. gefilterte Ansichten, Berichte, Verfahren oder Monitorsets. Normalerweise starten diese Objekte als private Objekte. Ein privates Objekt kann von keinem anderen Benutzer gesehen oder verwendet werden. Diese Benutzerobjekte können für andere *Benutzerrollen* oder einzelne *Benutzer* freigegeben werden. In manchen Fällen kann ein `Master`-Rollenbenutzer ein Benutzerobjekt öffentlich machen und allen Benutzern zur Verfügung stellen. Freigabeoptionen können das Recht zum Verwenden, Bearbeiten, Exportieren, Löschen oder Freigeben für andere Benutzer umfassen. Freigaberechte werden separat von jedem einzelnen Objekt eingerichtet. Sie können die Freigabe eines Benutzerobjekts für Folgendes wählen:

- Alle Benutzerrollen, deren Mitglied Sie sind. Dabei kommt es nicht darauf an, ob Sie diese Benutzerrolle gegenwärtig verwenden.
- Alle einzelnen Benutzer, die Mitglieder Ihres aktuellen Umfangs sind

Wenn Freigaberechte sowohl für die Benutzerrolle als auch einzelne Benutzer gewährt werden, werden die Freigaberechte zu einander hinzugefügt.

Normalerweise wird die Schaltfläche **Gemeinsam nutzen** auf einer Seite oder in einem Dialogfeld angezeigt, auf der/in dem ein Benutzerobjekt bearbeitet wird. Manchmal werden einzelne Schaltflächen **Gemeinsam nutzen** neben jedem Benutzerobjekt in einer Liste angezeigt.

Beispiele für Benutzerobjekte im VSA:

- Ansichtdefinitionen
- Installationspakete zur Agentbereitstellung
- Dashlet-Überwachung
- Agent-Verfahrensordner
- Service-Desk-Verfahrensordner
- Monitorsetordner
- SNMP-Satzordner
- Berichtsordner
- Berichtsgruppenordner
- Benannte Filter für **Service Desk**-Tickets

Hinweis: Ordnerstrukturen unterliegen speziellen Regeln zur gemeinsamen Nutzung von Ordnern. Einzelheiten finden Sie unter "Agent-Verfahren > Planen/Erstellen > **Ordnerrechte** *(siehe 125)*" in der Online-Benutzerhilfe.

Freigabeoptionen

Kaseya 2-Freigabeoptionen

- Durch Hinzufügen eines Benutzers oder einer Benutzerrolle zum **gemeinsam genutzten Feld** wird diesem Benutzer gestattet, dieses Objekt zu verwenden. Dem Benutzer bzw. der Benutzerrolle müssen keine zusätzlichen Rechte zugewiesen werden, um das Objekt zu verwenden.
- Durch Aktivieren *zusätzlicher Rechte* wie **Bearbeiten**, **Erstellen**, **Löschen**, **Umbenennen** oder **Gemeinsam nutzen** beim *Hinzufügen* des Benutzers oder der Benutzerrolle werden diesem Benutzer bzw. dieser Benutzerrolle die betreffenden zusätzlichen Rechte gewährt. Sie müssen den Benutzer oder die Benutzerrolle entfernen und erneut hinzufügen, um Änderungen an den zusätzlichen Rechten vorzunehmen.
- **Gemeinsam nutzen** bedeutet, dass die Benutzer oder Benutzerrollen Freigaberechte zuweisen können.

Alte Freigaberechte

Gewisse Funktionen in Kaseya 2 stellen die Freigaberechte immer noch mithilfe eines alten Dialogfeldes wie folgt ein:

- Freigaberechte werden *nach Objekt* zugewiesen. Es gibt drei Kontrollkästchenoptionen für die Freigabe. Die ersten beiden Kontrollkästchen *schließen einander aus* und bestimmen, welche Freigaberechte zugewiesen werden. Wird keins der beiden ersten Kontrollkästchen aktiviert, kann das Freigabeobjekt nur von den Benutzern gesehen werden, denen Freigabezugriff gewährt wurde. Das Objekt kann weder verwendet noch bearbeitet werden. Die Listenfelder **Freigegeben** und **Nicht freigegeben** und das dritte Kontrollkästchen bestimmen, wer das Objekt *sehen* kann.
  - **Anderen Administratoren gestatten zu ändern** – Wenn dies aktiviert ist, umfassen die Freigaberechte für das Objekt die Fähigkeit, es zu verwenden, seine Details anzuzeigen und es zu bearbeiten.
  - **Andere Administratoren dürfen verwenden, dürfen nicht anzeigen oder bearbeiten** – Wenn dies aktiviert ist, lassen die Freigaberechte für das Objekt nur dessen Verwendung zu.
  - **Als öffentlich festlegen (wird von allen Administratoren gesehen)** – Wenn dies aktiviert ist, wird sichergestellt, dass *alle* aktuellen und zukünftigen VSA-Benutzer das Objekt *sehen* können. Wenn es nicht aktiviert wird, können nur ausgewählte Benutzerrollen und Benutzer das Freigabeobjekt sehen. Wenn in diesem Fall später neue Benutzer oder Benutzerrollen hinzugefügt werden, müssen Sie zu diesem Dialogfeld zurückkehren und einstellen, dass sie das bestimmte Objekt sehen können.

Anmeldezeiten

System > Benutzersicherheit > Anmeldezeiten

Auf der Seite **Anmeldestunden** wird festgelegt, *wann* sich Benutzer beim VSA anmelden können, indem die Wochentage und Stunden für jede Benutzerrolle angegeben werden. Für jeden Tag der Woche können verschiedene Betriebsstunden eingestellt werden.

Hinweis: Eine Zusammenfassung der Funktionen, die sich auf Benutzeranmeldungen auswirken, finden Sie unter **Anmelderichtlinien für VSA** *(siehe 401)*.

Benutzerrolle auswählen

Wählen Sie eine **Benutzerrolle** *(siehe 382)* aus, um sie anzuzeigen und die Einstellungen ihrer Anmeldestunden zu pflegen.

Keine Zeitbeschränkung

Wenn dies aktiviert ist, können sich Benutzer an jedem Wochentag und zu jeder Uhrzeit beim VSA anmelden. Entfernen Sie die Markierung, um alle anderen Einstellungen zu aktivieren.

Ablehnen

Verweigert den Anmeldezugriff für den gesamten Wochentag.

oder zulassen zwischen <12:00> und <12:00>

Geben Sie den Uhrzeitbereich an, während dessen Anmeldungen erlaubt sind. Alle Uhrzeiten liegen in der Kaseya Server-Zeitzone. Stellen Sie Start- und Endzeit auf die gleiche Zeit ein, um Zugriff rund um die Uhr zu gestatten.

Benutzerhistorie

System > Benutzersicherheit > Benutzerhistorie

Auf der Seite **Benutzerhistorie** wird eine Historie (in Reihenfolge des Datums) jeder Funktion angezeigt, die von einem Benutzer verwendet wurde. Die Historie zeigt außerdem die vom **Systemprotokoll** *(siehe 442)* erfassten Aktionen an, die vom ausgewählten Benutzer ausgeführt wurden. Das System speichert die Historiendaten für jeden Benutzer für die Anzahl von Tagen, die für das **Systemprotokoll** festgelegt wurden.

Klicken Sie auf **einen Benutzernamen**, um das Protokoll für diesen Benutzer anzuzeigen.

> **Hinweis:** Diese Protokolldaten erscheinen in keinen Berichten.

Orgn./Gruppen/Abtlg./Personal

- **Verwalten** *(siehe 423)* – Erstellen Sie Organisationen, Rechnergruppen, Abteilungen und Mitarbeiter.
- **Typen einrichten** *(siehe 428)* – Erstellen Sie Organisationstypen zur Klassifizierung der Organisationen.

Verwalten

System > Orgn./Gruppen/Abtlg./Personal > Verwalten

Auf der Seite **Verwalten** werden die Organisationen definiert, zu denen Sie Geschäftsbeziehungen unterhalten. Eine Organisation ist typischerweise ein Kunde, kann jedoch auch ein Geschäftspartner sein. Organisationen werden mit **Scopes** *(siehe 419)*, Tickets und Desk-Definitionen verknüpft. Alle verwalteten Rechner, verwalteten Geräte und VSA-Benutzer gehören einer Organisation an.

Sie können Folgendes innerhalb einer Organisation definieren:

- **Allgemein** *(siehe 424)* – Allgemeine Einstellungen für die Organisation
- **Rechnergruppen** *(siehe 425)* – Mit dieser Organisation verknüpfte Rechnergruppen
- **Abteilungen** *(siehe 425)* – Eine Einheit der administrativen Zuständigkeit innerhalb einer Organisation
- **Mitarbeiter** *(siehe 426)* – Das einer Abteilung zugewiesene Personal
- **Benutzerdefinierte Felder** *(siehe 427)* – Weist benutzerdefinierten Feldern zur Klassifizierung von Organisationen Werte zu.

- **System-Management** *(siehe 427)* – Konfiguriert mithilfe eines Einrichtungsassistenten **Policy Management**-Richtlinien für eine Organisation.

Verwalten – Registerkarte "Allgemein"

System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Registerkarte ''Allgemein''

Klicken Sie auf **Neu**, um das Fenster **Organisation hinzufügen** anzuzeigen, oder klicken Sie auf eine Zeile im mittleren Feld und dann auf **Bearbeiten**, um das Fenster **Organisation ändern** anzuzeigen. Geben Sie die folgenden Attribute ein:

- **Neu/Konvertieren** – Wählen Sie **Neue Organisation**, wenn keine Datenquelle für die Konvertierung vorhanden ist. Wenn **Service Billing** installiert ist, können Sie eine Organisation erstellen, indem Sie einen bestehenden Kunden- oder Lieferantendatensatz **konvertieren** *(siehe 623)*.
- **ID** – Der Identifikator des Datensatzes. Kann nur über die Schaltfläche **Umbenennen** geändert werden.
- **Org.-Name** – Der Anzeigename für den Identifikator
- **Org.-Type** – Der Typ der Organisation. Siehe **Organisationstypen** *(siehe 428)*.
- **Standardabteilungsname** – Die Standardabteilung für die Organisation
- **Standardrechnergruppenname** – Die Standardrechnergruppe für die Organisation
- **Org.-Website** – Die Website der Organisation
- **Anzahl der Mitarbeiter** – Die Anzahl der Mitarbeiter in der Organisation
- **Jahresumsatz** – Der Jahresumsatz der Organisation
- **Bevorzugte Kontaktmethode** – Die bevorzugte Kontaktmethode der Organisation: `Phone, Email, Mail, Fax`.
- **Übergeordnete Organisation** – Die übergeordnete Organisation dieser Organisation. Diese muss vorher definiert worden sein, damit sie in dieser Dropdown-Liste angezeigt wird.
- **Primäre Telefonnummer** – Die Haupt-Telefonnummer der Organisation
- **Primäre E-Mail-Adresse** – Die Haupt-E-Mail-Adresse der Organisation
- **Hauptkontakt** – Der Hauptkontakt der Organisation. Ein Kontakt ist ein **Mitarbeiter** *(siehe 426)* einer Abteilung.
- Die Adresse der Organisation:
  - **Land**
  - **Straße**
  - **Stadt**
  - **US-Staat**
  - **Postleitzahl**
- **Karte** – Zeigt den Standort dieser Adresse in Google Maps an.

Es werden drei vordefinierte Organisationen bereitgestellt:

- `myOrg` ist die **Organisation** *(siehe 623)* des Dienstanbieters, der den VSA verwendet. Alle anderen Organisationen im VSA sind Fremdorganisationen, die mit `myOrg` geschäftliche Beziehungen unterhalten. Der Standardname `myOrg`, `My Organization`, sollte in den Firmennamen des Dienstanbieters umbenannt werden. *Dieser Name wird oben auf verschiedenen Berichten angezeigt, um dem Bericht ein Branding zu verleihen.* Agents, die auf intern verwalteten Rechnern installiert sind, können dieser Organisation zugewiesen werden. *VSA-Benutzeranmeldedaten sind üblicherweise mit Mitarbeiterdatensätzen in der Organisation* `myOrg` *verknüpft.* `myOrg` kann keiner übergeordneten Organisation zugeordnet werden.
- `Kserver` ist die Organisation, die den auf Ihrem Kaseya Server installierten Agents zugewiesen wird. Dies vereinfacht das Anwenden spezialisierter Einstellungen auf den Kaseya Server, dessen Pflege sich normalerweise von jener anderer von Agents verwalteter Rechner unterscheidet.

- `Unnamed` ist die Standardorganisation, die einem Agent zugewiesen wird. Die Pflege mehrerer Agent-Installationspakete in Agent > **Agents bereitstellen** *(siehe 40)*, einer für jede Organisation, kann sehr viel Zeit in Anspruch nehmen. Deshalb verwenden manche Serveranbieter ein einziges Agent-Paket für die `unnamed` Organisation und führen alle Installationen mithilfe dieses Pakets aus. System > **Benennungsrichtlinie** *(siehe 406)* kann der korrekten Organisations-Gruppen-ID automatisch neue Agents – und zwar beim ersten Check-in der Agents- auf Basis von IP oder Connection-Gateway jedes verwalteten Rechners zuweisen. Agent > **Einstellungen kopieren** *(siehe 62)* kann zu einem späteren Zeitpunkt geplant werden, um bestimmte Agent-Einstellungen nach **Rechner-ID-Vorlage** *(siehe 627)* auf den Rechnertyp zu kopieren, der von der Anfangsprüfung ermittelt wurde.

Verwalten – Registerkarte "Rechnergruppen"

System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Registerkarte "Rechnergruppen"

Definieren Sie die mit dieser Organisation verknüpften Rechnergruppen. Rechner werden immer nach Rechnergruppe definiert und Rechnergruppen stets nach Organisation. Sie können mehrere Hierarchieebenen von Rechnergruppe definieren, indem Sie eine übergeordnete Rechnergruppe für eine Rechnergruppe angeben.

Aktionen

- **Neu** – Fügt eine neue Rechnergruppe hinzu.
  - **Name** – Der Name der Rechnergruppe
  - **Übergeordnete Gruppe** – Die übergeordnete Rechnergruppe. Optional.
- **Rechnergruppen-ID umbenennen** – Ändert die ID der ausgewählten Rechnergruppe.
- **Verschieben** – Verschiebt alle Rechner und Unterrechnergruppen von einer Rechnergruppe in eine andere. Die Zielrechnergruppe kann in derselben oder in einer anderen Organisation liegen. *Die Ausgangsrechnergruppe wird nach dem Verschieben gelöscht.* Bei der letzten Rechnergruppe in einer Ausgangsorganisation ist kein Verschieben möglich.

> **Hinweis:** Wenn Sie dieselbe Rechnergruppe mit demselben Inhalt am Zielort erstellen möchten, erstellen Sie die neue Rechnergruppe am Zielort *vor* dem Verschieben und wählen Sie sie beim Verschieben aus.

- **Löschen** – Löscht die ausgewählte Rechnergruppe. Rechnergruppen dürfen keine Rechner mehr enthalten, um gelöscht werden zu können. Rechner können über "Agent > **Gruppe ändern** *(siehe 62)*" in eine andere Rechnergruppe verschoben werden.
- **Agents** – Listet die Rechner innerhalb der ausgewählten Rechnergruppe auf.
- **Standard einrichten** – Legt die ausgewählte Rechnergruppe als Standardrechnergruppe für die Organisation fest.

Verwalten – Registerkarte "Abteilungen"

System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Registerkarte ''Abteilungen''

Abteilungen können innerhalb einer Organisation oder eines Kunden- bzw. Anbieter-Datensatzes definiert werden. Beispiel: `IT`, `Sales` oder `Accounting`. Alle Mitarbeiter werden nach der Abteilung definiert, zu der sie gehören. Sie können mehrere Hierarchieebenen von Abteilungen definieren, indem Sie eine übergeordnete Abteilung für eine Abteilung angeben. Sie können einen Mitarbeiter einer beliebigen anderen Abteilung in derselben Organisation bzw. demselben Kunden- oder Anbieter-Datensatz zuweisen.

Aktionen

- **Neu/Bearbeiten** – Fügt eine neue Abteilung hinzu.
  - **Abteilungsname** – Der Name der Abteilung

- ➢ **Übergeordnete Abteilung** – Die übergeordnete Abteilung. Optional.
- ➢ **Manager** – Der Manager der Abteilung. Optional. Erfordert einen im Voraus definierten Mitarbeiterdatensatz.

- **Verschieben** – Verschiebt alle Mitarbeiter und Unterabteilungen von einer Abteilung in eine andere. Die Zielabteilung kann in derselben oder in einer anderen Organisation liegen. *Die Ausgangsabteilung wird nach dem Verschieben gelöscht.* Bei der letzten Abteilung in einer Ausgangsorganisation ist kein Verschieben möglich.

> **Hinweis:** Wenn Sie dieselbe Abteilung mit demselben Inhalt am Zielort erstellen möchten, erstellen Sie die neue Abteilung am Zielort *vor* dem Verschieben und wählen Sie sie beim Verschieben aus.

- **Abteilungs-ID andern** – Ändert die ID der ausgewählten Abteilung.
- **Löschen** – Löscht die ausgewählte Abteilung. Abteilungen dürfen keine Mitarbeiter mehr enthalten, um gelöscht werden zu können. Mitarbeiter können über die Registerkarte **Personal** *(siehe 426)* verschoben werden.
- **Als Standard festlegen** – Legt die ausgewählte Abteilung als Standardabteilung für die Organisation fest.
- **Löschen** – Löscht die ausgewählte Abteilung. Abteilungen dürfen keine Mitarbeiter mehr enthalten, um gelöscht werden zu können. Mitarbeiter können über die Registerkarte **Personal** *(siehe 426)* verschoben werden.

Verwalten – Registerkarte "Personal"

System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Registerkarte ''Personal''

Erstellen Sie Mitarbeiter in Abteilungen und pflegen Sie die Kontaktinformationen für jeden Mitarbeiter. Kontakte und deren Rufnummern können mit Tickets und Desk-Definitionen verknüpft werden. Die Mitarbeiterdaten können auch von Active Directory über "Agent > Domänen > **Domain-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#10750.htm)*" aktualisiert werden.

Mitarbeiterdatensatz hinzufügen/bearbeiten

- **Vollständiger Name** – Der volle Name einer Person in der Organisation
- **Abteilung** – Die Abteilung, mit der die Person verknüpft ist. Die Abteilung muss vorher definiert worden sein, damit sie in dieser Dropdown-Liste angezeigt wird.
- **Supervisor** – Die Person, an die dieser Mitarbeiter Bericht erstattet. Der Supervisor muss vorher als Mitarbeiter in derselben Abteilung definiert worden sein.
- **Titel** – Der Titel der Person in der Organisation
- **Funktion** – Die Funktion, in der die Person in der Organisation tätig ist
- **Telefonnummer** – Die direkte Telefonnummer der Person
- **E-Mail-Adresse** – Die E-Mail-Adresse der Person
- **Benutzername** – Die mit diesem Mitarbeiter verknüpfte VSA-Benutzer-ID. Erforderlich für die Funktionen **Alle Tickets anzeigen** und for Zeitüberwachung.
- **Alle Tickets anzeigen** – Wenn dies aktiviert ist, kann der mit diesem Mitarbeiter verknüpfte VSA-Benutzer alle **Service Desk**-Tickets in seinem Scope sowie die mit diesem spezifischen Mitarbeiterdatensatz verknüpften Tickets anzeigen. Wird diese Option nicht markiert, kann dieser VSA-Benutzer nur die mit diesem spezifischen Mitarbeiterdatensatz verknüpften **Service Desk**-Tickets anzeigen.

Bestätigung der Arbeitszeit

Ein Mitarbeiterdatensatz muss mit einem VSA-Benutzer verknüpft sein, damit Arbeitszeittabellen bestätigt werden können und Timer sichtbar sind.

- **Alle Arbeitszeittabellen bestätigen** – Wenn dies aktiviert ist, kann der Mitarbeiter alle Arbeitszeittabellen genehmigen. Dadurch wird sichergestellt, dass auch dann alle Arbeitszeittabellen rechtzeitig genehmigt werden, wenn Genehmiger gerade nicht verfügbar sind.
- **Bestätigungsmuster** – Gibt das Bestätigungsmuster an, das zur Genehmigung der Arbeitszeittabelle dieses Mitarbeiters erforderlich ist. Bestätigungsmuster geben an, ob die Genehmigung der Arbeitszeittabelle dieses Mitarbeiters durch dessen Supervisor oder wiederum dessen Supervisor (oder beiden) erfolgen muss.

Hinweis: Siehe Konfigurationsoptionen für Zeitüberwachung.

Sichtbarkeit von Service Desk-Tickets für einen Mitarbeiter

Wenn ein VSA-Benutzername mit dem Mitarbeiterdatensatz einer Organisation verknüpft ist, kann dieser VSA-Benutzer die mit diesem Datensatz verbundenen Tickets sehen, *selbst wenn der Scope des VSA-Benutzers dies nicht zulässt*. Alle von diesem VSA-Benutzer erstellten Tickets werden automatisch mit seinem Mitarbeiterdatensatz und seiner Organisation verknüpft. Diese Methode unterstützt hauptsächlich Rechnerbenutzer, die ihre eigenen Tickets über **Portalzugriff** *(siehe 75)* erstellen und verwalten. Rechnerbenutzer erwarten, Zugriff auf alle von ihnen und für sie erstellten Tickets zu haben. Eventuell wurden jedoch keine Umfangsberechtigungen für sie definiert. Wenn ein Scope für einen mit einem Mitarbeiter verknüpften VSA-Benutzer existiert, werden durch Aktivieren des Kontrollkästchens **Alle Tickets anzeigen** im **Mitarbeiterdatensatz** *(siehe 426)* diese zusätzlichen Tickets nach Scope sichtbar.

Beispiel: David ist der Hauptkundenkontakt für die XYZ-Organisation. Es wird ihm ein Umfang bereitgestellt, der ihm Sichtbarkeit aller Tickets für seine Organisation (selbst der nicht von ihm erstellten Tickets) gestattet, also ist das Kontrollkästchen **Alle Tickets anzeigen** aktiviert. Bernhard aus der XYZ-Organisation wendet sich an das Service-Desk, um ebenfalls ein Ticket einzureichen. Anfänglich ist es unklar, ob Bernhard Zugriff auf andere Tickets als die von ihm erstellten haben sollte, also ist das Kontrollkästchen **Alle Tickets anzeigen** nicht aktiviert. Wenn David zu einem späteren Zeitpunkt mehr Zugriffsrechte für Bernhard gewährt, kann das Service-Desk Bernhard einen Umfang zuweisen und das Kontrollkästchen **Alle Tickets anzeigen** aktivieren.

Verwalten – Registerkarte "Benutzerdefinierte Felder"

System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Registerkarte "Benutzerdefinierte Felder"

Weisen Sie den benutzerdefinierten Feldern auf dieser Registerkarte Werte zu. Diese Werte dienen der Klassifizierung von Organisationen. Die Namen der benutzerdefinierten Felder auf dieser Registerkarte können auf der Seite "Seitenanpassung > **Titel des benutzerspezifischen Org-Feldes** *(siehe 450)*" geändert werden.

Verwalten – Registerkarte "System-Management"

System > Orgn./Gruppen/Abtlg./Personal > Verwalten > Registerkarte ''System-Management''

Die Registerkarte **System-Management** enthält einen Einrichtungsassistenten. Mit dem Einrichtungsassistenten können Sie schnell *Rechnerverwaltungsrichtlinien für eine bestimmte Organisation konfigurieren und anwenden.* Sind die Richtlinien konfiguriert, werden diese auf alle Rechner angewandt, die Sie im Auftrag der betreffenden Organisation verwalten. Richtlinien bestimmen viele verschiedene Aspekte der Rechnerverwaltung:

- Audit-Planung
- Monitoring
- Benachrichtigungen
- Patch-Verwaltung
- Rechner-Routinewartung mithilfe von Agentverfahren

Dank der Richtlinien müssen Sie nicht mehr jeden Rechner einzeln verwalten. Sie müssen nur eine Richtlinie zuweisen oder ändern. Eine Richtlinienzuweisung oder -änderung im Rahmen einer zugewiesenen Richtlinie wird innerhalb von 30 Minuten an alle beteiligten Rechner verteilt, ohne dass Sie in die Planung eingreifen müssen. Danach können Sie leicht feststellen, ob ein verwalteter Rechner die zugewiesenen Richtlinien erfüllt oder nicht. Die Verfolgung der Erfüllung jeder einzelnen Richtlinie liefert Ihnen die Informationen, die Sie für die zuverlässige Bereitstellung von IT-Diensten für die gesamte von Ihnen betreute Organisation benötigen.

> **Hinweis:** Eine detaillierte Erläuterung der einzelnen Optionen im **Einrichtungsassistenten** *(http://help.kaseya.com/webhelp/DE/SSP/7000000/index.asp#11220.htm)* finden Sie in **Standard Solution Package**.

Arten einrichten

System > Orgn./Gruppen/Abtlg./Personal > Typen einrichten

Auf der Seite**Typen einrichten** werden Datensätze definiert, die Ihre Organisationen klassifizieren. Beispielsweise können Sie eine Organisation als `division`in Ihrem Unternehmen definieren oder Organisationen regional oder nach Umsatz klassifizieren. Andererseits können Sie Organisationen als `prospect`, `preferred customer` oder `business partner` einstufen. Das hängt von den Anforderungen in Ihrem Unternehmen ab.

Service-Desk

Typen einrichten kann optional auch zur automatischen **Verknüpfung eines Tickets mit einer Richtlinie** *(http://help.kaseya.com/webhelp/DE/KSD/7000000/index.asp#6210.htm)* im **Service Desk**-Modul genutzt werden.

Registerkarte "Allgemein"

Klicken Sie auf **Neu**, um das Fenster **Organisationstypen hinzufügen** anzuzeigen, oder klicken Sie auf eine Zeile im *mittleren* Feld und dann auf **Bearbeiten**, um das Fenster **Organisationstypen ändern** anzuzeigen. Geben Sie die folgenden Attribute ein:

- **ID** – Der Identifikator des Datensatzes. Dieser kann nicht mehr geändert werden, nachdem Sie ihn gespeichert haben.
- **Beschreibung** – Eine kurze Beschreibung dieser ID

Serververwaltung

Support anfordern

System > Serververwaltung > Support anfordern

Die Seite **Support anfordern** stellt mehrere Möglichkeiten zur Kontaktaufnahme mit dem Kaseya-Support zur Verfügung.

- **Support-Website** – Hier finden Sie Antworten auf allgemeine Fragen. Suchen Sie die Website für den Kaseya-Support unter **http://www.kaseya.com/support.aspx** *(http://www.kaseya.com/support.aspx)* auf. Diese Website stellt Links zum **Kaseya-Forum** und zur **Kaseya-Knowledge Base** bereit. Im Kaseya-Forum diskutiert eine interaktive Gemeinschaft von Kaseya-Nutzern täglich über eine Vielfalt von Themen und Lösungen. Lassen Sie sich im Forum eintragen, um interessante

Nachrichten zu erhalten, die direkt und up-to-date per E-Mail an Sie gesendet werden. Die Kaseya-Knowledge Base liefert technische Informationen über die Installation und Verwendung des IT Automation Framework von Kaseya.

- **Kaseya-Support Zugriff auf Ihr System gewähren** – Die Techniker des Kaseya-Supports können Probleme mit Ihrem System schnell und gründlich lösen, wenn sie direkten Zugriff auf Ihren Kaseya Server haben. Klicken Sie auf **Erstellen**, um ein `kaseyasupport`-Master-Benutzerkonto auf Ihrem System zu erstellen. Der Kaseya-Supporttechniker kann sich über unser System bei Ihrem System anmelden und helfen, irgendwelche Probleme zu lösen.

> **Hinweis:** Wir wissen, dass es beim Zugriff auf Ihren Kaseya Server Bedenken hinsichtlich der Sicherheit gibt. Zum Schutz der Anmeldung erstellt das System eine sicher Anmeldung. Niemand (nicht einmal der Kaseya-Supporttechniker) hat Zugriff auf dieses Passwort. Das Passwort wird bei jedem Klicken auf diese Schaltfläche geändert.

- **Klicken Sie hier, um Supportanfragen zu verwalten** – Das **Kaseya-Helpdesk** *(https://helpdesk.kaseya.com/home)* bietet eine einzige Kontaktstelle zur Verwaltung von Kaseya-Supporttickets, zum Zugriff auf die Knowledge Base und zur Teilnahme am Benutzerforum.

Ihre Daten

Normalerweise benötigt der Kaseya-Support einige grundlegenden Informationen über Ihr System, bevor die Hilfestellung eingeleitet werden kann. Ihr Benutzername, Ihre E-Mail-Adresse, Kunden-ID und System-URL werden zu Ihrem eigenen Nutzen bereitgestellt.

Konfigurieren

System > Serververwaltung > Konfigurieren

Auf der Seite **Konfigurieren** werden die Konfiguration Ihres Kaseya Server und verwandte Dienste verwaltet. Verwandte Themen:

- **Berichtskonfiguration ändern** *(siehe 434)*
- **Audit-Ergebnistabelle indizieren** *(siehe 437)*
- **Standard-Einstellungen** *(siehe 437)*
- **Kaseya Server Setup** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/Install)*

Version, Patch-Level und Lizenzierung

- **Versionsnummer** – Zeigt die Versionsnummer der Anwendung.
- **Installiertes Patch-Level** – Zeigt das installierte Patch-Level des Systems.
- **Verfügbares Patch-Level** – Zeigt das höchste verfügbare Patch-Level, das installiert werden kann.
- **Auf neueste Patches prüfen** – Klicken Sie auf diesen Link, um **Hinweise zum neuesten Patch** *(http://help.kaseya.com/webhelp/DE/RN/index.asp#PatchReleaseNotes.htm)* und Anweisungen zur Aktualisierung Ihres Systems zu erhalten.
- **Warnen, falls der Server keine Daten erhalten kann von http://vsaupdate.kaseya.net** – Aktivieren Sie dieses Kontrollkästchen, damit eine Warnung angezeigt wird, wenn Ihr VSA keine Verbindung mit `http://vsaupdate.kaseya.net` herstellen kann, um die aktuellste PCI-ID-Liste für das Audit abzurufen. Ihr System versucht, diese Informationen von `http://vsaupdate.kaseya.net` automatisch zu beschaffen. Überprüfen Sie, ob der Server über Port 80 eine ausgehende Verbindung mit `http://vsaupdate.kaseya.net` aufbauen kann und die Antwort nicht von Ihrer Firewall blockiert wird.
- **Warnung, wenn die Lizenz die maximale Anzahl an Arbeitsplätzen erreicht** – Aktivieren Sie dieses Kontrollkästchen, damit eine Warnung angezeigt wird, wenn die Anzahl der Rechner-ID-Konten die Höchstzahl für Ihren VSA erreicht.

Schema erneut anwenden/Datenbank defragmentieren

> **Warnung:** Wenden Sie den Microsoft-SQL-Optimierungsratgeber nicht auf das Schema an. Er fügt Tasten hinzu, die in Konflikt mit dem reibungslosen Betrieb des Systems stehen.

- Klicken Sie auf **Schema erneut anwenden**, um das letzte Datenbankschema, das über **Nach Aktualisierung suchen** heruntergeladen wurde, erneut zu installieren und zu bestätigen. "Schema erneut anwenden" ist ein sicherer Vorgang, der von Benutzern ausgeführt werden kann, um eine Vielzahl von Problemen zu lösen. Schema erneut anwenden:
  - Stellt Standardwerte ein und führt grundlegende Konsistenzprüfungen an der Datenbank aus.
  - Baut alle vordefinierten Kaseya-Verfahren erneut auf.
  - Baut alle vordefinierten Kaseya-Verfahrensbeispiele erneut auf.
  - Plant standardmäßige Back-End-Verarbeitungsverfahren für den Kaseya Server neu.
  - Wird nur dann automatisch ausgeführt, wenn der Kaseya Server aktualisiert oder ein Zusatzmodul installiert wird.

    All dies wird ohne Risiko des Verlusts von Agentdaten ausgeführt. Dies ist eine gute Selbstbehebungsroutine, falls Sie Folgendes bemerken:
  - Verfahren schlagen in der **FALLS**-Bedingung oder in bestimmten Schritten fehl.
  - Anstehende Meldungen werden nicht in einem zweiminütigen Intervall verarbeitet. Sie können dies auf der Seite "System > **Statistiken** *(siehe 442)*" überwachen. Dies könnte auf ein Problem mit Back-End-Verarbeitungsverfahren hinweisen.
- Klicken Sie auf **Datenbank defragmentieren**, um die physischen Dateien auf Ihren Platten-Arrays zu defragmentieren. Fragmentierte SQL-Serverdatendateien können den E/A-Zugriff verlangsamen.

Beispieldaten

- **Beispiel-Skripts mit allen Aktualisierungen und Datenbank-Wartungszyklus neu laden** – Aktivieren Sie diese Option, um Beispiel-Agent-Verfahren neu zu laden.
- **Beispiel-Ereignissätze mit allen Aktualisierungen und Datenbank-Wartungszyklus neu laden** – Aktivieren Sie diese Option, um Beispiel-Ereignissätze neu zu laden.
- **Beispiel-Monitorsets mit allen Aktualisierungen und Datenbank-Wartungszyklus neu laden** – Aktivieren Sie diese Option, um Beispiel-Monitorsets neu zu laden.

HTTPS

- **Automatisch zu https auf der Anmeldeseite umleiten (außer bei Zugriff über localhost)** – Wenn dies aktiviert ist, wird sichergestellt, dass alle Benutzer, die sich remote beim VSA anmelden, das sichere HTTPS-Protokoll verwenden.

API

- **VSA-API-Web-Service aktivieren** – Aktivieren Sie diese Option, um den **VSA-API-Web-Service** *(siehe 532)* zu aktivieren.

Patch-Verwaltung

- **Benachrichtigungen über ungültige Patch-Speicherorte** – Manchmal bereitet Microsoft Patches vor, die es der Funktion Dateiquelle nicht gestatten, Patches erfolgreich herunterzuladen. Wenn diese Option aktiviert ist, wird Kaseya darüber benachrichtigt, dass ein "ungültiger Patch-Speicherort" für ein Patch existiert, das von den verwalteten Rechnern in Ihrem System benötigt wird. Die Benachrichtigung meldet Kaseya, einen gültigen Patch-Speicherort manuell vorzubereiten und diesen als aktuelle Patch-Speicherortüberschreibung zur Verwendung von allen Kunden zu senden. Wird diese Option nicht aktiviert, wird keine Benachrichtigung an Kaseya gesendet. Ungeachtet dieser Einstellung erhalten Sie dennoch aktualisierte

Patch-Speicherortüberschreibungen, die als Reaktion auf Benachrichtigungen durch *andere* Kunden vorbereitet wurden.

> **Hinweis:** Die Benachrichtigung sendet keine kunden- oder rechnerspezifischen Informationen an Kaseya.

Ticketing

- **Nicht authentifizierten Benutzern erlauben, Anhänge aus Ticketbenachrichtigungen herunterzuladen** – Wenn dies aktiviert ist, können in den Anmeldungen zu Tickets eingebettete Links zu Anhängen in ausgehenden E-Mails geöffnet werden, ohne dass der Benutzer sich beim VSA authentifizieren muss. Aus Sicherheitsgründen wird von der Aktivierung dieser Option abgeraten.

Datenbank-Backups

- **Datenbank-Backup/-Wartung laufen lassen alle<N> Tage um <Uhrzeit>** – Der Kaseya Server sichert und pflegt die MS-SQL-Datenbank und das Transaktionsprotokoll automatisch. Klicken Sie auf **Periode einstellen**, um die ausgewählte Häufigkeit und Uhrzeit einzustellen. Wenn Ihr Kaseya Server zur geplanten Sicherungszeit abgeschaltet ist, wird die Sicherung das nächste Mal ausgeführt, wenn der Kaseya Server online ist. Sie können eine Null eingeben, um periodische Sicherungen zu deaktivieren.
- **Backup-Ordner auf KServer** – Stellen Sie den Verzeichnispfad zum Speichern der Datenbanksicherungen ein. Normalerweise lautet der Standardpfad `C:\Kaseya\UserProfiles\@dbBackup`. Klicken Sie auf **Ändern**, um Änderungen am Verzeichnispfad zu bestätigen. Klicken Sie auf **Standard**, um den Verzeichnispfad auf seine Standardeinstellung zurückzusetzen.

> **Hinweis:** Datenbanken, die älter als dreimal die Sicherungs- und Wartungsperiode sind, werden automatisch gelöscht, um ein Überfüllen des Plattenlaufwerks zu verhindern. Wenn die Sicherung beispielsweise alle 7 Tage ausgeführt wird, werden alle Sicherungen, die älter als 21 Tage sind, gelöscht.

- **DB ändern** – Verbinden Sie Ihren Kaseya Server mit einer Datenbank auf einem anderen Rechner.
  1. Sichern Sie Ihre vorhandene `ksubscribers`-Datenbank über die Option **Jetzt sichern** auf der Seite "System > Konfigurieren".
  2. Kopieren Sie die Datenbanksicherungsdatei auf den Datenbankserver, mit dem Sie eine Verbindung herstellen möchten.
  3. Stellen Sie die `ksubscribers`-Datenbank auf dem neuen Datenbankserver mit SQL Server Management Studio (SSMS) wieder her. Klicken Sie mit der rechten Maustaste auf "Datenbanken > Datenbank wiederherstellen…"
  4. Stellen Sie sicher, dass die wiederhergestellte `ksubscribers`-Datenbank auf **Authentifizierung im gemischten Modus** gesetzt ist.
     - ✓ Klicken Sie in SQL Server Management Studio (SSMS) mit der rechten Maustaste auf die wiederhergestellte `ksubscribers`-Datenbank und wählen Sie **Eigenschaften**.
     - ✓ Klicken Sie auf die Registerkarte **Sicherheit**.
     - ✓ Wählen Sie unter "Authentifizierung" **SQL-Server und Windows** aus.
     - ✓ Klicken Sie auf **OK**.
  5. Vergewissern Sie sich, dass auf dem neuen Datenbankserver **CLR aktiviert ist** *(https://helpdesk.kaseya.com/entries/33743166)*.
  6. Stellen Sie sicher, dass sich Ihr Kaseya Server im selben LAN wie der neue Datenbankserver befindet und **Port 1433** auf dem Datenbankserver geöffnet ist.
  7. Klicken Sie auf die Schaltfläche **DB ändern**.
  8. Geben Sie den Speicherort der Datenbank in einem der folgenden Formate ein:

- ✓ Computername
- ✓ Computername\Instanzname
- ✓ IP-Adresse

9. Geben Sie einen Datenbankanmeldenamen ein. Der standardmäßige Anmeldename lautet `sa`.

> **Hinweis:** Dieser Anmeldename wird nur zum Konfigurieren der Datenbank verwendet. Das System erstellt später seinen eigenen Anmeldenamen.

10. Geben Sie das mit diesem Anmeldenamen verknüpfte Passwort ein.
11. Klicken Sie auf **Anwenden**. Das System stellt dann eine Verbindung mit der Remote-Datenbank her und konfiguriert sie.

- **Jetzt sichern** – Leiten Sie sofort eine vollständige Datenbanksicherung ein. Verwenden Sie diese Funktion, *bevor* Sie den Kaseya Server herunterfahren oder migrieren, um sicherzustellen, dass die aktuellsten Kaseya Server-Daten in einer Sicherungskopie gespeichert werden. Die Sicherung wird geplant, innerhalb der nächsten 2 Minuten ausgeführt zu werden.
- **Wiederherstellen** – Klicken Sie, um die Kaseya Server-Datenbank aus einer Sicherungsdatei wiederherzustellen. Ein Dateibrowser zeigt eine Liste der Kaseya Server-Sicherungsdateien an, die zur Wiederherstellung zur Verfügung stehen.

> **Hinweis:** Nach Wiederherstellung einer 5.1-Datenbank wird die SSRS-URL ungültig und muss zurückgesetzt werden. Nach Wiederherstellung einer 6.x-Datenbank wird die SSRS-URL möglicherweise ungültig und muss zurückgesetzt werden.

Archiv

Die Archivierung von Agent-Protokollen nach Protokoll und Rechner-ID wird über "Agent > **Protokollhistorie** *(siehe 36)*" aktiviert.

- **Protokolle jeden Tag archivieren und endgültig löschen um <Uhrzeit>** – Geben Sie die Tageszeit an, zu der Protokolldateien archiviert und gelöscht werden.
- **Periode einstellen** – Klicken Sie, um die Änderung der Uhrzeit zu bestätigen, zu der Protokolldateien archiviert und gelöscht werden.
- **Pfad des Protokolldateiarchivs** – Dies ist der Dateispeicherort für die Archivdateien.

> **Hinweis:** Die Protokollarchive der Monitoring-Daten auf der Seite "Agent > **Protokollhistorie** *(siehe 36)*" werden im Verzeichnis `<KaseyaRoot>\UserProfiles\@dbBackup` gespeichert. Damit soll die Leistung von Systemen verbessert werden, bei denen sich die Datenbank auf einem anderen Server befindet. Alle anderen Agent-Protokollarchive werden in dem im Feld "System > **Konfigurieren** *(siehe 429)* > **Pfad des Protokolldateiarchivs**" angegebenen Verzeichnis gespeichert.

- **Ändern** – Klicken Sie, um das Ändern des Speicherorts für die Archivdateien zu bestätigen. Es wird ein Verfahren ausgeführt, um alle vorhandenen Archivdateien vom alten Speicherort an den neuen zu verschieben.
- **Standard** – Setzt den Pfad des Protokolldateiarchivs auf den Standardspeicherort auf dem Kaseya Server zurück. Es wird ein Verfahren ausgeführt, um alle vorhandenen Archivdateien vom alten Speicherort an den neuen zu verschieben.

Serverstatus

- **KServer-Protokoll** – Zeigt die letzten 300 kB der Kaseya Server-Protokolldatei an. Die gesamte Protokolldatei nimmt bis zu 5 MB ein und wird unter `xx\KServer\KServer.log` gespeichert, wobei `xx` das übergeordnete Verzeichnis des VSA-Webverzeichnisses darstellt.

- **Live-Connect KServer** – Ein Agent ist automatisch auf dem Kaseya Server installiert. Sie können auf das Check-in-Symbol dieses Agent klicken, um eine **Live-Connect** *(siehe 393)*-Sitzung mit dem Kaseya Server zu starten.
- **KServer anhalten** – Zeigt den aktuellen Status des Kaseya Server: **läuft** oder **gestoppt**. Der Kaseya Server kann durch Klicken auf **Dienst anhalten** angehalten werden.
- **Alarmauslösung aktivieren** – Deaktivieren Sie dieses Kontrollkästchen, um unnötige Alarme zu verhindern. Alarme können ausgelöst werden, wenn Sie den Kaseya Server anhalten, die Verbindung mit dem Internet trennen oder das System pflegen. Lassen Sie dieses Kontrollkästchen ansonsten aktiviert.
- **MsgSys neu starten** – Der MessageSys-Dienst wird neu gestartet. Dieser Dienst ist der Anwendungsserver, der Anfragen von VSA-Anwendungsbenutzern verwaltet.
- **Protokollierung von Verfahrensfehlern mit Markierung "Verfahren fortsetzen, falls Schritt fehlschlägt" aktivieren** – Wenn dies aktiviert ist, werden fehlgeschlagene Schritte in Verfahren protokolliert. Ist diese Option nicht aktiviert, werden fehlgeschlagene Schritte in Verfahren *nicht* protokolliert.
- **Protokollieren für erfolgreiche Ausführung von untergeordnetem Script in Agent-Verfahrensprotokoll aktivieren** – Wenn diese Option nicht aktiviert ist, wird die erfolgreiche Ausführung von untergeordneten Scripts nicht in das **Agent-Verfahrensprotokoll** *(siehe 35)* aufgenommen. Damit kann die Größe des Agent-Verfahrensprotokolls drastisch reduziert werden. Es dauert bis zu 5 Minuten, bis der KServer diese Einstellungsänderungen gelesen hat.
- **Autom. Schließen für Alarme und Tickets aktivieren** – Wenn diese Option aktiviert ist, werden offene Alarme und Tickets für Monitor-Sets und Offline-Meldungen automatisch geschlossen, wenn die Meldungsbedingung nicht mehr gegeben ist. Offline-Meldungen werden mithilfe von Agent-Status-Meldungen konfiguriert. Damit dieses Kontrollkästchen aktiviert werden kann, muss das Kontrollkästchen **Alarmauslösung aktivieren** aktiviert sein.

Server-Einstellungen

- **Zeitformat auswählen** – Klicken Sie auf das entsprechende Optionsfeld, um auszuwählen, wie die Uhrzeit angezeigt wird. Der Standard ist das AM/PM-Format. Beide Anzeigeformate sind mit Microsoft Excel kompatibel.
  - AM/PM-Format – 9:55:50 pm 9-Apr-07
  - 24-Stunden-Format – 21:55:50 9-Apr-07

> **Hinweis:** Das Uhrzeit-Offset wird unter "System > **Voreinstellungen** *(siehe 402)*" festgelegt. Das Datumsformat wird unter "System > **Lokale Einstellungen** *(siehe 452)*" eingestellt.

- **Externen Namen / IP-Adresse des Servers ändern** – Zeigt den aktuellen externen Namen oder die IP-Adresse des Kaseya Server an. Dies ist die Adresse, auf die die Agents auf verwalteten Rechnern zu Check-in-Zwecken zugreifen. Die Adresse kann geändert werden, indem Sie eine neue Adresse oder einen neuen Hostnamen in das Feld eingeben und auf **Namen/IP ändern** klicken.

> **Hinweis:** Verwenden Sie *keinen* Computernamen für den Kaseya Server. Der Agent verwendet standardmäßige WinSock-Aufrufe, um eine IP-Adresse aus einem **vollständig qualifizierten Hostnamen** aufzulösen. Die IP-Adresse wird von NETBIOS aus einem Computernamen aufgelöst. Dies ist eventuell nicht auf jedem Computer aktiviert. NETBIOS ist eine optionale letzte Methode, die Windows zum Auflösen eines Namens einsetzt. Daher werden nur vollständig qualifizierte Namen oder IP-Adressen unterstützt.

- **URL auf MS-SQL-Reporting-Services-Engine setzen** – Klicken Sie auf **Berichtskonfiguration ändern** *(siehe 434)*, um die URL anzugeben, über die sich der VSA mit Reporting Services verbindet. Sie können auch die Anmeldedaten für den Zugriff auf Reporting Services angeben und die URL ändern, die in der Kopfzeile aller VSA-Berichte angezeigt wird.

- **Serverport, über den die Agents einchecken, angeben mit** – Wenn Sie einen anderen Port eingeben und auf **Port ändern** klicken, wird der vom Kaseya Server verwendete Port *sofort* gewechselt.

> **Warnung:** Stellen Sie vor dem Ändern des Kaseya Server-Ports sicher, dass alle Agents so eingestellt sind, dass sie den neuen Port mit ihrem primären oder sekundären Kaseya Server verwenden. Agent-Check-ins werden über "Agent > **Check-in-Kontrolle** *(siehe 68)*" konfiguriert.

- **KServer-ID** – Die ID, über die Agents an den Kaseya Server gebunden werden. Das ist der eindeutige Bezeichner für diesen Kaseya Server. Gebundene Agents können erst dann einchecken, wenn die eindeutige Kaseya Server-ID, an die sie über "Agent > **Check-in-Kontrolle** *(siehe 68)*" gebunden wurden, der eindeutigen ID des Kaseya Server unter "System > **Konfigurieren** *(siehe 429)* > **ID ändern**" entspricht. Dadurch wird das Spoofing der IP-Adresse durch Umleitung von Agent-Check-ins verhindert.Ändern Sie die Kaseya Server-ID nur, wenn Sie einen aktualisierten VSA installieren und die ID eines bestehenden Kaseya Server mit bereits gebundenen Agents duplizieren möchten.

Versionsinformationen

Zeigt die folgenden Informationen über Ihre VSA-Konfiguration an.

- Betriebssystemversion
- IIS-Version
- Kaseya Server-Version
- SQL-Version
- Datenbankspeicherort
- Agent auf Kaseya Server

Referenzen

- **Versionsanmerkungen** – Klicken Sie auf **Versionsanmerkungen**, um eine Liste aller am VSA vorgenommenen Änderungen und Verbesserungen für alle Softwareversionen anzuzeigen.
- **Lizenz zeigen** – Klicken Sie auf **Lizenz zeigen**, um die aktuelle Lizenzvereinbarung zur Verwendung des VSA anzuzeigen.

Berichtskonfiguration ändern

System > Serververwaltung > Konfigurieren *(siehe 429)* > Berichtskonfiguration ändern

Im Dialogfeld **Berichtskonfiguration ändern** wird der Typ des Berichtsservers ausgewählt, der die Berichte ausführt.

- Der integrierte proprietäre Berichtsserver bedarf keiner weiteren Konfiguration.
- Wenn Sie stattdessen SQL Server Reporting Services (SSRS) verwenden möchten, können Sie die Verbindung zwischen VSA und der SSRS-Instanz zur Generierung von VSA-Berichten konfigurieren. Der SSRS kann lokal oder remote aus dem Kaseya Server und lokal oder remote aus der SQL-Serverinstanz, auf der die `ksubscribers`-Datenbank gehostet wird, installiert werden.

Aktionen

- **Bearbeiten** – Bearbeitet die Konfiguration des Berichtsservers.
- **Test** – Testet, ob die Konfiguration des Berichtsservers ordnungsgemäß funktioniert.
- **Registrierung ausführen** – Entwickler können hiermit neu erstellte **Datensätze** *(siehe 192)* für benutzeranpassbare Berichte registrieren, anstatt **Schema erneut anwenden** im gesamten VSA ausführen zu müssen.

Optionen

- **Kaseya-Berichtserstellung verwenden** – Wenn aktiviert, wird der integrierte proprietäre Berichtsserver zum Ausführen von Berichten verwendet. Dies ist hauptsächlich für kleinere Implementierungen des VSA gedacht. Dieser Berichtsserver wird standardmäßig für Neuinstallationen des VSA verwendet. Wenn die Option nicht ausgewählt ist, wird stattdessen ein SSRS-Berichtsdienst verwendet. SSRS ist für größere Implementierungen geeignet. Wenn nicht ausgewählt, müssen Sie eine URL für den **Hostnamen** der Instanz der SQL Server Reporting Services angeben, um Berichte ausführen zu können.
- **Berichtserstattungs-Zeitlimit (Min.)** – Legt die Zeit fest, die bis zur Fertigstellung der Publizierung verstreichen darf.
- **Hostname** – Die URL, die vom VSA für die Verbindung mit der Instanz der SQL Server Reporting Services verwendet wird. Muss zur Ausführung angegeben werden. Der VSA nutzt zur Verbindung mit der Instanz der SQL Server Reporting Services üblicherweise eines der nachfolgenden URL-Muster. Die Angabe der korrekten URL ist verpflichtend.

  > **Hinweis:** Eine visuelle Anleitung der zu Konfiguration eines SSRS-Berichtsservers notwendigen Schritte finden Sie unter **Kaseya Server-Setup** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/install/index.asp#home.htm)*.

  SQL an derselben Box wie VSA

  `http://localhost/ReportServer` *(am gängigsten)*
  `http://localhost/ReportServer$SQLExpress`
  `http://localhost/ReportServer$<SQLINSTANCENAME>` *(2005)*
  `http://localhost/ReportServer_<SQLINSTANCENAME>` *(2008)*
  `http://localhost:<PORTNUMBER>/ReportServer$<SQLINSTANCENAME>` *(2005)*
  `http://localhost:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME>` *(2008*

  SQL-Box separat vom VSA

  `http(s)://<SQLSERVERNAME>/ReportServer` *(am gängigsten)*
  `http(s)://<SQLSERVERNAME>/ReportServer$SQLExpress`
  `http(s)://<SQLSERVERNAME>/ReportServer$<SQLINSTANCENAME>` *(2005)*
  `http(s)://<SQLSERVERNAME>/ReportServer_<SQLINSTANCENAME>` *(2008)*
  `http(s)://<SQLSERVERNAME>:<PORTNUMBER>/ReportServer$<SQLINSTANCENAME>` *(2005)*
  `http(s)://<SQLSERVERNAME>:<PORTNUMBER>/ReportServer_<SQLINSTANCENAME>` *(2008)*
- **Benutzername** – Der Benutzername, der bei der Ausführung von Berichten für den Zugriff auf die Reporting-Services-Instanz verwendet wird. Gilt für einige Konfigurationen. Nähere Informationen erhalten Sie im Abschnitt **Benutzername** unten.
- **Logo** – Die URL des in der Kopfzeile der Berichte angezeigten Bilds. Gilt für einige Konfigurationen. Standardmäßig zeigen VSA-Berichtskopfzeilen das unter "System > Seitenanpassung > **Website-Kopfzeile** *(siehe 448)*" angegebene Bild an. Durch Änderung des Werts in "System > Konfigurieren > **Berichtskonfiguration ändern** *(siehe 434)* > **Logo**" können Sie diese Standardeinstellung überschreiben und die URL *nur für Berichtskopfzeilen ändern*. Die Änderung der URL im Feld "Berichtskonfiguration ändern > **Logo**" wirkt sich nicht auf das Bild in der **Website-Kopfzeile** aus. Wenn in SSRS-Berichten kein Logo angezeigt wird, kann dies folgende Gründe haben:
  - Der SSRS ist auf demselben Rechner wie der Kaseya Server installiert. SSRS kann das Logo aufgrund von Firewall-Problemen nicht abrufen. Ändern Sie die URL von der extern verfügbaren URL/IP-Adresse zu `localhost`.
  - Der VSA wurde unter Verwendung eines selbstsignierten SSL-Zertifikats konfiguriert. Ändern Sie das Protokoll von `https` zu `http`.
- **Berichts-URL-Basis** – Überschreibt die für CURL-Berichte verwendete URL. Bei den meisten Berichten wird zur Erstellung die *externe*VSA URL herangezogen, aber bei CURL-Berichten kann ein Problem namens "Router Loopback" auftreten. Um dies zu vermeiden, geben Sie eine andere URL als die externe VSA-URL an. Wird standardmäßig auf `http://localhost:80/` gesetzt.

- **Simultane Berichte** – Legt die Anzahl der Berichte fest, die gleichzeitig publiziert werden können. Bei Überschreitung dieser Anzahl werden die restlichen Berichte in die Warteschlange gestellt.
- **Alle Berichte behalten** – Wenn `No`, bestimmt die **Anzahl der Tage** den Zeitraum der Aufbewahrung. Wenn `Yes`, werden alle Berichte beibehalten und die Einstellung **Anzahl der Tage** spielt keine Rolle.
- **Anzahl der Tage behalten** – Legt die Anzahl der Tage fest, für die ein Bericht nach seinem Erstellungsdatum aufbewahrt wird. Muss mindestens 30 Tage betragen.

> **Hinweis:** Es werden nur Berichte gelöscht, die *nach* der Aktivierung der Option **Anzahl der Tage** erstellt wurden. Berichte können manuell im Verzeichnis `<Kaseya_Installation_Directory>\WebPages\DataReports` gelöscht werden.

Benutzername

Sie können allen VSA-Benutzern Anmeldedaten zur Verfügung stellen, anhand derer sie SSRS-Berichte ausführen können. Dadurch entfällt die Notwendigkeit, Zugriffsrechte für jeden VSA-Benutzer einzurichten, der Zugriff auf die SSRS benötigt. Dies gilt insbesondere für VSA-Benutzer in einer Arbeitsgruppe statt einer Domain, die über kein zentralisiertes Authentifizierungsverfahren wie etwa Active Directory zur Verwaltung der Zugriffsrechte auf die SSRS verfügen.

Anmeldedaten werden an drei verschiedenen Orten festgelegt:

- Benutzerkonten im Hostsystem des SSRS.
- SSRS Report Manager.
- VSA > System> Konfigurieren > URL ändern > Benutzername

Dieses Verfahren erstellt einen dedizierten Benutzer – in diesem Beispiel `KaseyaReport` – im Hostsystem des SSRS. Im SSRS **Report Manager** wird dem `KaseyaReport`-Benutzer die Ausführung von Berichten im SSRS ermöglicht. Abschließend werden die `KaseyaReport`-Anmeldedaten unter "System> Konfigurieren > URL ändern" registriert. > Benutzername-Felder. Ab diesem Punkt verwendet der VSA diese Anmeldedaten zum Zugriff auf die SSRS, wann immer ein VSA-Benutzer einen Bericht ausführt.

1. Fügen Sie im Hostsystem des SSRS einen `KaseyaReport`-Benutzer über die **Microsoft Management Console** hinzu. In der Microsoft Management Console können Sie die nachfolgenden Kontrollkästchen für den neuen Benutzer aktivieren oder deaktivieren.
   - Geben Sie ein starkes Passwort für den Benutzer ein.
   - Deaktivieren Sie das Feld **User must change password at next logon**.
   - Aktivieren Sie die Felder **User cannot change password** und **Password never expires**.
2. Erteilen Sie dem neuen Benutzer die erforderlichen Berechtigungen für Ihre Umgebung.
3. Öffnen Sie auf dem Hostsystem des SSRS einen Browser und geben Sie die URL für **Report Manager** (z. B. `http://localhost/Reports`) über das `Administrator`-Konto ein.
4. Klicken Sie auf **Site Settings** in der oberen rechten Ecke.
5. Klicken Sie in der linken Seitenleiste auf **Sicherheit** .
6. Klicken Sie auf **New Role Assignment** in der Menüleiste.
7. Geben Sie den in Schritt 1 erstellten Benutzernamen in das Feld **Gruppen- oder Benutzername** ein, z. B. `KaseyaReport`.
8. Aktivieren Sie das Kontrollkästchen **Systembenutzer**.
9. Klicken Sie auf **Hinzufügen**.
10. Öffnen Sie im VSA die Seite "System > Serververwaltung > **Konfigurieren**". Klicken Sie auf die Schaltfläche **URL ändern**, um das Dialogfeld zu öffnen.
11. Klicken Sie oben auf der Seite auf die Schaltfläche **Edit**.
12. Geben Sie die in Schritt 1 definierten Anmeldedaten ein, und stellen Sie sicher, dass das Kontrollkästchen **Specify Account** aktiviert ist. Dies bedeutet, dass SSRS die von Ihnen

eingegebenen Anmeldedaten verwendet. Falls der Benutzer, etwa `KaseyaReport`, kein Domänenbenutzer ist, können Sie das Feld **Domäne** leer lassen.

13. Klicken Sie auf **Save** und dann auf die Schaltfläche **Test**, um die Änderungen zu testen.

Audit-Ergebnistabelle indizieren

Hinweis: Die folgende einmalige Konfiguration muss nur dann vorgenommen werden, wenn ein Dialogfeld die Indizierung der Audit-Ergebnistabelle empfiehlt. Wenn überhaupt, wird dieses Dialogfeld nur angezeigt, wenn ein Master-Benutzer sich beim VSA anmeldet.

Die Indizierung der Audit-Ergebnistabelle kann die Reaktionszeit der Kaseya Server-Datenbank verbessern. **Abhängig von der Anzahl der Datensätze in der Tabelle kann dieser Vorgang 1 bis 4 Stunden dauern. Der Kaseya Server sollte während dieses Prozesses heruntergefahren werden, um einen möglichen Verlust der Audit-Daten zu vermeiden.**

1. Klicken Sie auf der Seite "System > **Konfigurieren** *(siehe 429)*" auf **KServer anhalten**.
2. In SQL Server Management Studio:
   a. Öffnen Sie ein neues Abfragefenster und stellen Sie sicher, dass `ksubscribers` die ausgewählte Datenbank ist.
   b. Führen Sie die folgende gespeicherte Prozedur aus: `Exec spCreateAuditRsltAppsPK`
   Dies kann zwischen 1 und 4 Stunden oder sogar noch länger dauern, je nach Anzahl der Datensätze in der Tabelle und der Geschwindigkeit des SQL-Servers.
3. Klicken Sie auf der Seite "System > **Konfigurieren** *(siehe 429)*" auf **KServer starten**.

Hinweis: Indizes in der `ksubscribers` -Datenbank manuell oder über den SQL-Optimierungsratgeber zu erstellen kann zu Fehlern bei der Neuanwendung des Schemas und dem Upgrade auf neuere Versionen von Kaseya führen. Es wird daher dringend davon abgeraten.

Standard-Einstellungen

System > Serververwaltung > Standard-Einstellungen

Auf der Seite **Standard-Einstellungen** werden die Standard-Einstellungen für die Serververwaltung sowie eine Positivliste für den Dateiupload eingerichtet.

Registerkarte "Standard-Einstellungen"

- **Standardzeit für Zeitplan** – Legt die Standardzeit fest, die für die Planung verwendet wird: **Zeitplanung nach Agent-Zeit** *(siehe 624)* oder Zeitplanung nach Serverzeit. Gilt nur Scheduler, die Zeitplanung nach Agent-Zeit unterstützen.
- **Ermittlung – Domain Watch-Richtlinie "Neue Rechner/Kontakte einschließen" schließt verschobene Objekte ein** – Wenn auf einen OU/Container eine Richtlinie mit aktivierten Optionen "Neue Rechner einschließen" oder "Neue Kontakte einschließen" angewendet wird und:
  - Diese Option "Y" lautet, wird die Richtlinie auf Computer und Kontakte angewendet, die in den OU/Container verschoben werden.
  - Diese Option "N" lautet, wird die Richtlinie nicht auf Computer und Kontakte angewendet, die in den OU/Container verschoben werden.
- **Ermittlung – Mitarbeiterdatensatz "Alle Tickets anzeigen" aktiviert** – Wenn dies aktiviert ist, wird das Kontrollkästchen **Alle Tickets anzeigen** *(siehe 426)* bei der Erstellung des Mitarbeiterdatensatzes aktiviert.
- **Ermittlung – Mitarbeiterdatensatz Abteilungs-Namenszuweisungsschema**
  - `Assign based on Active Directory OU Name` – Für den neuen Mitarbeiterdatensatz wird anhand des OU/Container-Namens eine Abteilung erstellt.

- `Assign based on Active Directory Department property` – Für den neuen Mitarbeiterdatensatz wird anhand des Abteilungsnamens, der in Active Directory für den Benutzer angegeben ist, eine Abteilung erstellt.

- **Ermittlung – Mitarbeiterdatensatz Mitarbeiter-Namenszuweisungsschema**
  - `Assign based on Active Directory Display name. If empty, use First name plus Last name`
  - `Assign based on Active Directory User logon name`
  - `Assign based on Active Directory First name plus Last name`
- **LAN-Cache – Automatisch generierte Anmeldedaten verwenden** – Wenn ja, werden beim Erstellen eines LAN-Cache über das Dialogfeld "Agent > Agent-Einstellungen konfigurieren > **LAN-Cache** *(siehe 78)* > LAN-Cache hinzufügen" automatisch Anmeldedaten erstellt. Wenn nein, können Sie im selben Dialogfeld manuell bestehende Anmeldedaten für den neu erstellten LAN-Cache festlegen.
- **E-Mail-Adresse bei Anmeldung erforderlich** – Wenn ja und wenn für einen Benutzer keine definierte E-Mail-Adresse vorliegt, muss der Benutzer bei der Anmeldung sofort eine E-Mail-Adresse angeben. Wenn nein, ist die E-Mail-Adresse optional.
- **E-Mail-Adresse erforderlich für Benutzername** – Wenn ja, muss ein Benutzernamen-Datensatz eine E-Mail-Adresse aufweisen. Wenn nein, ist die E-Mail-Adresse optional.
- **Organisationen in Ansichten mit einer Rechnergruppe anzeigen** – Steuert die Anzeige der Dropdown-Liste **Rechnergruppe** am oberen Rand aller Agent-Seiten. Wenn `Y`, zeigt die Dropdown-Liste **Rechnergruppe** jede Organisation und Rechnergruppe als eigenen Eintrag an. Wenn `N`, werden *nur Organisationen mit nur einer Rechnergruppe* nicht als eigene Einträge in der Liste geführt.

  > **Hinweis:** Wenn Sie mit dem **Ticketing-Modul** arbeiten und Tickets nach Organisation zuweisen, sollte diese Option auf `N` gesetzt werden.

- **Bei Erstellung von Benutzerpasswörtern Domänenkurznamen verwenden** – Wenn Legacy-AD-Anmeldedaten über die Seite **AD-Benutzer anzeigen** in VSA 6.2 oder früher erstellt wurden und weiterhin verwendet werden, wählen Sie `Yes`. Damit stellen Sie sicher, dass die Passwörter in bestehenden Legacy-AD-Anmeldedaten weiterhin erkannt werden. Bei jeder Zurücksetzung des Passworts in bestehenden AD-Anmeldedaten wird ein neuerer, auf vollständig qualifizierten Domänennamen basierender Hash-Algorithmus verwendet. Wenn Legacy-AD-Anmeldedaten aus der Seite **AD-Benutzer anzeigen** vor 6.3 niemals implementiert wurden, wählen Sie "Nein".

Registerkarte "Datei-Upload-Positivliste"

Die Registerkarte **Datei-Upload-Positivliste** legt fest, welche Art von Dateianhängen in die verschiedenen **Rich-Text-Editoren** *(siehe 162)* im gesamten VSA-Framework hochgeladen werden dürfen. Hier geben Sie einen Standardsatz von Dateitypen an. Die Standarddateitypen können zwar gelöscht, aber nicht bearbeitet werden. Benutzer können die Liste zurücksetzen, sodass ausschließlich die Standarddateitypen zugelassen werden. Nur Benutzer mit Master-Rolle haben Zugriff auf diese neue Registerkarte.

Tickets aus **Service Desk** und **Ticketing**, die durch eingehende E-Mails generiert werden, akzeptieren nur Anhänge mit den auf dieser Registerkarte zugelassenen Dateierweiterungen. Wenn bei der Verarbeitung einer eingehenden E-Mail-Nachricht ein Dateianhang nicht akzeptiert wird, wird in die Beschreibung des Tickets eine Nachricht mit dem Hinweis, dass der Dateianhang entfernt wurde, und eine Liste der zulässigen Dateierweiterungen eingefügt.

Lizenzmanager

System > Serververwaltung > Lizenzmanager

Auf der Seite **Lizenzmanager** werden Rechnerlizenzen nach Organisations-ID oder Gruppen-ID zugewiesen. Außerdem wird auf dieser Seite die Anzahl der Lizenztypen angezeigt, die für jeden

Rollentyp erworben wurden. Sie können Benutzersitzungen gegebenenfalls über diese Seite beenden, damit sich andere Benutzer anmelden können.

Die Typen der verwalteten Lizenzen umfassen Folgendes:

- Agent-Lizenzen – Gelten für Rechner nach Organisation, Gruppe oder Gruppen-ID
- Rollentyplizenzen – Gelten für VSA-Benutzer oder -Rechner nach Rollentyp.

Die Zusatzmodul-Lizenzen werden nur angezeigt, wenn Sie diese Zusatzmodule erworben und installiert haben.

Agent-Lizenzzahlen

Die folgenden Ereignisse wirken sich auf Agent-Lizenzzahlen aus:

- Eine "nicht verwendete" Agent-Lizenz wird in "verwendet" geändert, wenn ein Rechner-ID-Konto erstellt und der Agent installiert wird.
- Falls der Agent, aber nicht das Konto, gelöscht wird, wird die Agent-Lizenz dennoch als "verwendet" betrachtet.
- Wenn das Konto gelöscht wird (ungeachtet dessen, was mit dem Agent geschieht), erhält die Agent-Lizenz wieder den Status "nicht verwendet".
- Falls ein Konto erstellt wird, der Agent jedoch noch nicht zum ersten Mal installiert ist, wird das Konto als **Rechner-ID-Vorlage** *(siehe 627)* bezeichnet. Rechner-ID-Kontovorlagen werden erst als "verwendet" gezählt, wenn Sie den Agent installieren.

Registerkarte "Allgemein"

Auf der Registerkarte **Allgemein** werden die von Ihnen erworbenen Produkte angezeigt.

Aktualisierungscode...

Klicken Sie auf **Aktualisierungscode...**, um einen neuen Lizenzcode einzugeben oder Ihren existierenden Lizenzcode erneut anzuwenden.

Lizenz zeigen

Klicken Sie auf **Lizenz zeigen**, um die aktuelle Lizenzvereinbarung zur Verwendung des VSA anzuzeigen.

(Kopfzeileninformationen)

Zeigt die folgenden Informationen über Ihre VSA-Konfiguration an.

- **Managed Services Edition von Kaseya** – Die Versionsnummer des Kaseya Server
- **Lizenzcode** – Der aktuelle Lizenzcode für diesen Kaseya Server
- **Ablaufdatum** – Das aktuelle Ablaufdatum für die Ausführung des Systems im "Ist"-Zustand mit dem aktuellen Lizenzcode
- **Ablaufdatum der Wartungslizenz** – Das aktuelle Ablaufdatum der Wartungsdienste, einschließlich Upgrades und Zugang zum technischen Support

Tabelle der Produktnamen

Zeigt die folgenden Informationen über Ihre Zusatzmodule an.

- **Produktname** – Die Versionsnummer des Kaseya Server
- **Version** – Die Versionsnummer des Produkts
- **Status** – Der Status des Produkts: `Installed`.
- **Aktuelle Hotfix-Ebene** – Die aktuelle Hotfix-Ebene für das Zusatzmodul
- **Nutzungstyp** – Die für das Produkt aktivierte Funktionalitätsebene. Gilt für alle Rollentypen. Siehe Service Desk-Lizenzierung.

Registerkarte "Lizenzen"

Auf der Registerkarte **Lizenzen** wird die Anzahl der Agent-basierten Lizenzen für jedes von Ihnen erworbene Produkt angezeigt. Sie können Anteile der Gesamtzahl an Agent-Lizenzen, die Sie für ein Produkt erworben haben, einer spezifischen Organisation und bestimmten Rechnergruppen zuweisen.

(Tabelle der Lizenztypen)

Die Tabelle der Lizenztypen zeigt Folgendes an:

- **Lizenztyp** – Führt jedes von Ihnen erworbene Produkt an, das eine Agent-basierte Lizenz benötigt. Dies kann Folgendes umfassen:
  - Agents – VSA-Agents
  - KBU – Arbeitplatzrechner-Clients
  - KBU – Serverclients
  - KES – Endpoint Security-Clients
  - KDPM – Desktop Management-Clients
- **Verwendet** – Die aktuelle Anzahl der verwalteten Rechner, auf denen dieses Produkt installiert ist
- **Max** – Die Höchstanzahl der verwalteten Rechner, auf denen dieses Produkt installiert werden kann

Lizenzzuweisungen ändern

Die Gesamtanzahl der verfügbaren Lizenzen kann einer spezifischen Organisation, Gruppe oder Untergruppen-ID zugewiesen werden. Wählen Sie eine Organisation, Gruppe oder Untergruppe aus der Zuweisungstabelle aus und klicken Sie dann auf die Schaltfläche **Lizenzzuweisungen ändern**.

(Zuweisungstabelle)

Die Zuweisungstabelle zeigt Folgendes an:

- **Organisation/Rechnergruppe** – Listet sowohl Organisationen als auch Gruppen in Organisationen in einer einzigen Spalte auf. Sie wählen eine Zeile aus, um ihr Agent-Lizenzen zuzuweisen.
- **Typ** – `Org` oder `Group` Rechnergruppen können Rechneruntergruppen enthalten.
- **Verwendete Agents** – Die aktuelle Anzahl der verwalteten Rechner, auf denen dieses Produkt in dieser Organisation oder Rechnergruppe installiert ist
- **Max. Agents** – Die aktuelle Anzahl der verwalteten Rechner, auf denen dieses Produkt in dieser Organisation oder Rechnergruppe installiert werden kann

Registerkarte "Rollentypen"

Auf der Registerkarte **Rollentypen** wird die Zahl der Lizenzen angezeigt, die Sie für jeden Rollentyp in Ihrem VSA erworben haben. Kaseya-Lizenzen werden nach Rollentyp erworben. Es gibt separate Rollentypen zur Lizenzierung von Benutzern nach *Benutzerrollentyp* und zur Lizenzierung von Rechnern nach *Rechnerrollentyp*. Die einzelnen Rollen ermöglichen die Nutzung festgelegter Funktionen, die unter "Benutzerrollen > **Zugriffsrechte** *(siehe 415)*" bzw. "Rechnerrollen > **Zugriffsrechte** *(siehe 418)*" aufgelistet sind. Die Anzahl der erworbenen Rollentyplizenzen wird auf der Registerkarte "System > **Lizenzmanager** *(siehe 438)* > Rollentyp" angezeigt. Jede Rollentyplizenz gibt die Anzahl der zulässigen *genannten Benutzer* und *gleichzeitigen Benutzer* an.

- **Rollentyp** – Der Name des Rollentyps
- **Beschreibung** – Die Beschreibung des Rollentyps
- **Max. benannte Lizenzen** – Die Höchstanzahl der Benutzer, die für diesen Rollentyp lizenziert wurden
- **Max. gleichzeitige Lizenzen** – Die Höchstanzahl der gleichzeitigen Benutzer, die für diesen Rollentyp lizenziert wurden

Sitzungen anzeigen

Klicken Sie auf einen Rollentyp und dann auf **Sitzungen anzeigen**, um eine Liste der aktuellen VSA-Benutzersitzungen anzuzeigen, die diesen Rollentyp verwenden. Sie können eine oder mehrere Sitzungen auswählen und auf **Ausgewählte Sitzungen abmelden** klicken, um diese Sitzungen zu beenden. Verwenden Sie diese Funktion, um unnötige Sitzungen abzumelden, wenn ein Benutzer sich nicht anmelden kann, weil ein Rollentypmaximum von *gleichzeitigen* Sitzungen erreicht wurde.

Import-Center

System > Serververwaltung > Import-Center

Auf der Seite **Import-Center** werden Automatisierungslösungen, d. h. benutzerdefinierte Datenstrukturen, die auf mehrere Agents angewendet werden können, in den VSA importiert und daraus exportiert. Dadurch erhalten Sie die Möglichkeit, Automatisierungslösungen von einem VSA auf einen anderen zu migrieren oder Automatisierungslösungen von anderen Anbietern zu importieren. Folgende Import- bzw. Exporttypen von Automatisierungslösungen werden unterstützt:

- Pakete
- Agent-Verfahren – Beinhaltet die Option zum Export und Import von Ordnern mit Agent-Verfahren. Aktivieren Sie am oberen Rand des Dialogfelds **Neuer Export** das Kontrollkästchen **Nur Ordner anzeigen**, um einen *Ordner* mit zu exportierenden Agent-Verfahren anzugeben.
- Agent-Vorlagen
- Ereignis-Sätze
- Service-Desk-Feiertage
- Monitor-Sets
- Monitor-SNMP-Sets
- Patch-Richtlinien
- Richtlinie
- Berichte
- Berichtsdatenteil
- Berichtsvorlage
- Service-Desk-Tickets
- Service-Desk-Definitionen
- Service-Desk-Mitteilungsvorlagen
- Ansichten

Sie können in einer einzigen XML-Datei mehrere Elemente unterschiedlicher Typen importieren oder exportieren. Es kann beispielsweise vorkommen, dass sie einen Satz von Agent-Verfahren sowie Monitor-Sets importieren möchten, die gemeinsam eine Automatisierungslösung darstellen.

Registerkarte "Importe"

Über diese Registerkarte können Sie eine XML-Datei einer Automatisierungslösung in Ihren VSA importieren.

- **Neuer Import** – Wählen Sie die gewünschte XML-Datei aus und klicken Sie auf **Verarbeiten**.
- **Import-Daten ansehen** – Zeigt die Importhistorie an.

Die Seite enthält ein Protokoll der importierten Dateien.

Registerkarte "Exporte"

Über diese Registerkarte können Sie eine XML-Datei einer Automatisierungslösung aus Ihrem VSA exportieren.

- **Neuer Export**
  1. Wählen Sie den Typ der Automatisierungslösung aus, der exportiert werden soll.

2. Sie können dabei einen oder mehrere Typ(en) gleichzeitig auswählen.
3. **Klicken Sie auf die Schaltfläche Weiter, um einen weiteren Typ von Automatisierungslösung auszuwählen.**
4. Klicken Sie zum Exportieren auf die Schaltfläche **Exportieren**. Eine einzelne XML-Datei wird erstellt, die immer noch auf dem Kaseya Server gespeichert ist.
5. Klicken Sie auf den Hyperlink der neu exportierten Datei, der in der Tabelle auf der Seite "Exporte" angezeigt wird.
6. Bestätigen Sie die Speicherung der Datei auf Ihrem lokalen Rechner.

- **Exportangaben anzeigen** – Zeigt die Exporthistorie an.

Systemprotokoll

System > Serververwaltung > Systemprotokoll

Auf der Seite **Systemprotokoll** werden Ereignisse protokolliert, die nicht nach Rechner-ID für einen festgelegten Zeitraum verfolgt werden können. *Dieses Protokoll erfasst Ereignisse, die in keinem der Agent-Protokolle enthalten sind.* Beispiele:

- Löschen von Rechner-IDs
- Fehlgeschlagene und erfolgreiche Anmeldeversuche
- Erfolgreiche Kaseya-Remote-Control-Sitzungen
- Starten/Anhalten des Kaseya Server
- Löschen von Trouble Tickets, die einer Gruppe (nicht einem Rechner) zugewiesen wurden
- Planen von Berichten

Historie speichern für N Tage

Klicken Sie auf **Anwenden**, um Systemprotokollereignisse für die angegebene Zahl von Tagen zu speichern.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Suchen

Die Suchfunktion agiert als Filter im Feld **Beschreibung**. Geben Sie eine Gruppe von Wörtern ein, nach denen gesucht werden soll, und klicken Sie auf die Schaltfläche **Suchen**. Es werden nur Zeilen angezeigt, die mit den Suchkriterien übereinstimmen. Verwenden Sie % oder * als Platzhalterzeichen. Verwenden Sie das Unterstrichzeichen (_) als Platzhalterzeichen für ein einzelnes Zeichen. Bei dem Text muss auf Groß- und Kleinschreibung geachtet werden.

> **Hinweis:** Diese Protokolldaten erscheinen in keinen Berichten.

Statistiken

System > Serververwaltung > Statistiken

- Zugehörige Informationen werden über "Berichte > Netzwerkstatistiken *(siehe 208)*" bereitgestellt.

Auf der Seite **Statistiken** sehen Sie verschiedene Statistiken, um die optimale Ausführung des Kaseya Server zu überprüfen. Die Einstellung **Rechner-ID-ID/Gruppen-ID-Filter** *(siehe 626)* hat keinerlei Auswirkung auf die gezeigten Statistiken.

Agents derzeit online

Die Anzahl der Agents, die gegenwärtig im System einchecken

Gesamtzahl verwendeter Lizenzen

Die Anzahl der verwendeten Agent-Lizenzen

Gesamtzahl der Vorlagenkonten

Die Anzahl der definierten **Rechner-ID-Vorlagen** *(siehe 627)*

Die Gesamtzahl der Rechner-IDs

Die Anzahl der auf dem Kaseya Server definierten Rechner-IDs, egal, ob ihre Agents jemals eingecheckt haben oder nicht.*Gesamtzahl der verwendeten Lizenzen + Gesamtzahl der Vorlagenkonten = Gesamtzahl der Rechner-IDs.*

Nutzung der Kserver-CPU

die letzten 5 Minuten: x%
Langzeitdurchschnitt: x%

Gesamtnutzung der System-CPU

die letzten 5 Minuten: x%
Langzeitdurchschnitt: x%

Remote-Control-Sitzungen

Die Anzahl der durch den Kaseya Server geleiteten Remote-Control-Sitzungen, die gegenwärtig aktiv sind

Anstehende Meldungen

Meldungen werden alle zwei Minuten von der Hintergrundaufgabe verarbeitet. Diese Zahl zeigt, wie viele aufgestaute Meldungen darauf warten, vom System verarbeitet zu werden. Wenn mehr als 0 Meldungen anstehen, wird eine Schaltfläche mit der Bezeichnung **Meldungen löschen** angezeigt. Klicken Sie auf diese Schaltfläche, um alle anstehenden Meldungen zu löschen.

Offene Patch-Scan-Ergebnisse

Dies ist die Anzahl der Rechner, die gegenwärtig über Patch-Scanergebnisse verfügen, die zwar abgeschlossen aber noch nicht verarbeitet wurden. Wenn ein Kaseya Server viele Patch-Scans aufweist, die in einem kurzen Zeitraum ausgeführt werden, werden die tatsächlichen Ergebnisse dieser Scans eventuell erst nach langer Zeit angezeigt. Die Zählung ist ein Maß des Verarbeitungsrückstands.

Datenbankspeicherort

Zeigt den Speicherort der Datenbank an.

Datenbankgröße

Die Gesamtgröße Ihrer Datenbank. Typische Systeme verbrauchen ungefähr 1 bis 2 MB an Datenbankgröße pro Rechner-ID.

Datenbankdateipfad

Der vollständige Pfad zur Datenbank auf dem Datenbankserver-Rechner

Kaseya Dateipfad

Der vollständige Pfad auf dem Kaseya Server zum Speicherort der Systemdateien

Statistiken erfasst

- **Aktive Verbindungen** – Die Anzahl der verwalteten Rechner, die gegenwärtig aktive Verbindungen mit dem Kaseya Server unterhalten

- **Neue Verbindungen in den letzten 10 Sekunden** – Die Anzahl der neuen TCP/IP-Verbindungen, die vom Kaseya Server akzeptiert wurden. Agent, die während eines früheren Check-in eine Verbindung herstellten, werden hierbei nicht gezählt.
- **Warteschlangenlänge der Check-in-Nachrichten** – Die Anzahl der Check-in-Nachrichten, die auf die Verarbeitung durch den Kaseya Server warten
- **Warteschlangenlänge der Befehlsnachrichten** – Die Anzahl aller Nachrichten außer Check-in-Nachrichten, die auf die Verarbeitung durch den Kaseya Server warten
- **Bandbreite – erhalten Byte/s** – Byte-pro-Sekunde-Input am Kaseya Server-Agent-Port
- **Bandbreite – gesendet Byte/s** – Byte-pro-Sekunde-Output am Kaseya Server-Agent-Port
- **Nutzung der Datenbank-CPU –** Diese Zahl gibt den Prozentsatz der CPU-Nutzung durch den Datenbankserver zur festgelegten Zeit an. Übermäßig hohe Werte für längere Perioden könnten bedeuten, dass dieser Server untermotorisiert ist oder von zusätzlichem RAM profitieren könnte.
- **Anzahl der verarbeiteten Verbindungen seit dem KServer-Start –** Anzahl der gesamten Agent-Verbindungen, die seit dem letzten Start des Diensts vom Kaseya Server verarbeitet wurden
- **Ereignisprotokolleinträge erhalten in letzter Minute** – Die Anzahl der Ereignisprotokolleinträge, die in der letzten Minute für das ganze System erhalten wurden
- **Ereignisprotokolleinträge erhalten in letzen 5 Minuten** – Die Anzahl der Ereignisprotokolleinträge, die in den letzten 5 Minuten für das ganze System erhalten wurden
- **Ereignisprotokolleinträge erhalten in letzer Stunde** – Die Anzahl der Ereignisprotokolleinträge, die in der letzten Stunde für das ganze System erhalten wurden

In der letzten Stunde gelaufene Spitzenverfahren

Diese Tabelle führt die Verfahren auf, die auf allen Online-Rechnern in der letzten Stunde ausgeführt und abgeschlossen wurden. Die höchste Häufigkeit wird zuerst aufgelistet.

Anstehende Spitzenverfahren (nur Online-Rechner)

Diese Tabelle führt die Verfahren auf, die auf die Ausführung auf allen Online-Rechnern warten. Die höchste Häufigkeit wird zuerst aufgelistet.

Anmelderichtlinie

System > Serververwaltung > Anmelderichtlinie

Auf der Seite **Anmelderichtlinie** werden für alle VSA-Benutzer gültige Anmelderichtlinien eingerichtet. Anmelderegeln verhindern einen gewaltsamen Einbruch in das System. Durch Beschränken der aufeinander folgenden fehlerhaften Anmeldeversuche und Deaktivieren von Rogue-Konten für einen festgelegten Zeitraum können Sie unbefugten Zugriff verhindern, der durch Eingabe von willkürlichen Passwörtern erlangt wird.

> **Hinweis:** Eine Zusammenfassung der Funktionen, die sich auf Benutzeranmeldungen auswirken, finden Sie unter **Anmelderichtlinien für VSA** *(siehe 401)*.

Bestimmen Sie die Richtlinie zu ungültigen Anmeldeversuchen

- **Anzahl der nicht erfolgreichen Anmeldeversuche in Folge, bevor das Konto gesperrt wird** – Geben Sie die Anzahl der fehlerhaften Anmeldungen an, die einem VSA-Benutzer oder **Portalzugriff** *(siehe 75)*-Benutzer hintereinander gestattet sind, bevor sein Konto im Feld "Konto" deaktiviert wird. Nach einer erfolgreichen Anmeldung wird die Zählung auf Null zurückgesetzt.
- **Zeitdauer, nach der das Konto deaktiviert wird, nachdem die Höchstanzahl der fehlgeschlagenen Anmeldeversuche überschritten wurde** – Geben Sie die Zeitdauer in Stunden oder Tagen an, während der das Konto im Feld "Konto" deaktiviert bleibt.

> **Hinweis:** Um das Konto manuell vor Verstreichen der Sperrzeit zu aktivieren, muss ein anderer Benutzer das Konto über die Seite "System > **Benutzer** *(siehe 409)*" aktivieren.

- **Minuten der Inaktivität, bevor eine Benutzersitzung abläuft**– Geben Sie die Dauer der Benutzerinaktivität an, bevor der Benutzer automatisch abgemeldet wird. Stellen Sie die Minuten der Inaktivität im Feld ein.
- **Verhindern, dass Personen ihren Anmeldenamen ändern** – Verhindern Sie, dass eine Person ihren Anmelde*namen* ändert.
- **Domain auf der Anmeldeseite nicht anzeigen** – Blenden Sie das Feld **Domain** auf der Anmeldeseite aus.

> **Hinweis:** Wenn das Kontrollkästchen "Domäne" nicht markiert wird, wird es erst auf der Anmeldeseite angezeigt, wenn zumindest eine Domänenanmeldung existiert. Domänenanmeldungen können über "Agent > AD-Benutzer anzeigen" importiert oder manuell über "System > **Login ändern** *(siehe 404)*" hinzugefügt werden.

- **Das Kontrollkästchen 'Remember me' bei der Anmeldung nicht anzeigen** – Blenden Sie das Kontrollkästchen **Meinen Benutzernamen auf diesem Computer speichern** auf der Anmeldeseite aus.

Geben Sie eine Richtlinie für die Passwortsicherheit an

Legen Sie eine Passwortstärke fest, indem Sie die Kontrollkästchen neben Folgendem aktivieren:

- **Erfordert Passwortänderung alle N Tage**
- **Mindestlänge des Passworts erzwingen**
- **Passwortwiederholung verbieten für N Passwörter**
- **Groß- und Kleinbuchstaben erforderlich**
- **Sowohl Buchstaben als auch Zahlen erforderlich**
- **Nicht-alphanumerische Zeichen erforderlich**

Aktualisieren

Klicken Sie auf **Aktualisieren**, um die Einstellungen anzuwenden.

Anwendungsprotokollierung

System > Serververwaltung > Anwendungsprotokollierung

Die Seite **Anwendungsprotokollierung** dient der Protokollierung von Anwendungsaktivität auf dem Anwendungsserver. *Diese Funktion wird nur für Benutzer mit Master-Rolle angezeigt und hauptsächlich vom Kaseya-Support verwendet.*

- Die Protokollierungsebenen in den Protokolldateien können von `None` bis `Maximum` eingestellt werden. Die Informationsmenge in diesen Protokollen hängt vom Umfang der Protokollierung in jeder Anwendung und der in der Konfiguration der **Anwendungsprotokollierung** festgelegten Detailebene ab.
- Anhand der bereitgestellten Kontrollkästchen können Sie die Anfrage und die Reaktion aufzeichnen. In `\Kaseya>Xml>Log` wird eine XML-Datei für jede Anfrage und jede Reaktion erstellt. Darüber hinaus gibt es eine Option für die Transaktionsprotokollierung. Wenn diese Option aktiviert ist, wird für jede Datenbankaktualisierung eine weitere XML-Datei im selben Verzeichnis erstellt.
- Es gibt Optionen zum Filtern nach Warteschlange. Damit kann die im Protokoll verzeichnete Informationsmenge eingeschränkt werden.
- Die Registerkarte **Protokoll** zeigt Protokolleinträge an. Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(siehe 18)*.

Ausgehende E-Mail

System > Serververwaltung > Ausgehende E-Mail

Auf der Seite **Ausgehende E-Mail** werden Einstellungen für das Routen von ausgehenden E-Mails vom Kaseya Server an einen Host-E-Mail-Server gepflegt. Der Host-E-Mail-Server akzeptiert ausgehende E-Mail-Nachrichten und sendet diese für Sie an die Empfänger. Falls der Host-E-Mail-Server eine Authentifizierung erfordert, können Sie einen Benutzernamen und ein Passwort einschließen.

> **Hinweis:** Diese Einstellungen werden normalerweise während der Installation festgelegt. Sie können nach der Installation mithilfe dieser Seite geändert werden.

Automatische Zustellung aktivieren/deaktivieren

Die automatische Zustellung ausgehender E-Mail-Nachrichten ist standardmäßig deaktiviert. Sie müssen die automatische Zustellung ausgehender E-Mail-Nachrichten im gesamten VSA aktivieren, sobald die Nachrichten erstellt wurden.

Manuelle Zustellung

Sie können selbst bei deaktivierter automatischer Zustellung E-Mail-Nachrichten senden:

1. Klicken Sie auf die Registerkarte "System > Ausgehende E-Mail > **Protokoll**".
2. Wählen Sie eine oder mehrere ausgehende E-Mail-Nachricht(en) mit dem Status `Queued` aus.
3. Klicken Sie auf die Schaltfläche **Jetzt senden**.

Konfiguration

Klicken Sie auf **Bearbeiten**. Füllen Sie die Felder im Dialogfeld **Bearbeiten** aus.

- **Hostname** – Der Name des Host-E-Mail-Servers, Beispiel: `smtp.mycompany.com`. Wenn keine Authentifizierung oder keine spezielle Portnummer erforderlich ist, geben Sie nur Werte für die Felder **Standardaufbewahrungstage für Protokolle** und **Standardabsender** an.

  > **Hinweis:** Die Eingabe von `localhost` im Feld **Hostname** bedeutet, dass Sie den virtuellen **Standard-IIS-SMTP-Server** des Kaseya Server zum Routen der ausgehenden E-Mail-Nachrichten verwenden. Der **virtuelle Standard-SMTP-Server**-Dienst muss installiert und ausgeführt werden, um E-Mail-Nachrichten zu senden Außerdem muss der Dienst DNS-Adressen auflösen können, um E-Mail-Nachrichten an andere SMTP-Server zu senden.

- **Port** – Dies ist normalerweise 25, aber der Host-E-Mail-Server erfordert eventuell eine andere Portnummer. Die Ports 465 und 587 werden üblicherweise für die Verbindung mit einem SMTP-Mailserver über SSL/TLS verwendet.
- **Benutzername** – Wenn dieser für die Authentifizierung erforderlich ist, geben Sie den Benutzernamen eines Kontos ein, das zur Verwendung des Host-E-Mail-Servers befugt ist.
- **Passwort** – Falls dieses für die Authentifizierung erforderlich ist, geben Sie das Passwort des Kontos ein.
- **Standardaufbewahrungstage für Protokolle** – Geben Sie die Anzahl der Tage ein, für die ausgehende E-Mail-Einträge aufbewahrt werden sollen.
- **Standardmäßige Absender-E-Mail** – Geben Sie die Standardadresse "Von" ein, die in der ausgehenden E-Mail-Nachricht angezeigt wird. Die von der ausgehenden E-Mail-Nachricht angezeigte "Von"-Adresse verwendet die folgende Rangordnung:
  1. Wenn eine Von-Adresse im Verfahrensschritt **sendEmail()** vorhanden ist, wird diese Adresse verwendet.
  2. Ansonsten wird in diesem Schritt die Von-Adresse verwendet, die von einer verknüpften "Service-Desk > **Nachrichtenvorlage**" bereitgestellt wurde (vorausgesetzt, der Link existiert und es wurde eine Von-Adresse angegeben).

3. Ist dies nicht der Fall, verwendet dieser Verfahrensschritt die **Antwort-E-Mail-Adresse** des mit dem Service-Desk unter "Service Desk > **Einstellungen für eingehende E-Mails und Alarme** > E-Mail-Leseprogramm" verknüpften E-Mail-Leseprogramms. Diese Verknüpfung zwischen Leseprogramm und Service-Desk wird unter "Service-Desk > Desk-Definition > Eigenschaften > Allgemein > Standardfeld-Standardwerte > E-Mail" eingestellt.
4. Ansonsten wird die **Standardabsender-E-Mailadresse** verwendet, die unter "System > **Ausgehende E-Mail**" festgelegt ist.

Testen

Wenn Sie den Verdacht haben, keine E-Mail-Nachrichten vom Kaseya Server zu erhalten, klicken Sie auf die Schaltfläche **Test** auf dieser Seite, um Test-E-Mail-Nachrichten an verschiedene Empfängeradressen zu senden.

> **Hinweis:** Bei Eingabe von `localhost` in das Feld **Hostname** kann es vorkommen, dass auf der Registerkarte **Protokoll** der erfolgreiche Versand der E-Mail-Nachricht angegeben wird, auch wenn sie aufgrund von Konfigurationsproblemen mit dem **virtuellen Standard-SMTP-Server** nicht erfolgreich weitergeleitet werden konnte.

Klicken Sie auf **Testen**. Füllen Sie die Felder im Dialogfeld **Testen** aus.

- **An** – Die E-Mail-Adresse, an die die Test-E-Mail-Adresse gesendet wird
- **Betreff** – Die Betreffzeile der Test-E-Mail-Nachricht

Protokollierung

Auf der Registerkarte **Protokoll** wird ein Protokoll aller ausgehender E-Mail-Nachrichten angezeigt, die vom Kaseya Server gesendet wurden. Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(siehe 18)*.

- **Jetzt senden** – Senden Sie ausgewählte E-Mail-Nachrichten oder senden Sie diese erneut.
- **Weiterleiten** – Leiten Sie eine ausgewählte E-Mail-Nachricht an eine andere Adresse als ursprünglich angegeben weiter.
- **Anzeigen** – Zeigen Sie eine ausgewählte E-Mail-Nachricht an.
- **Löschen** – Löschen Sie ausgewählte E-Mail-Nachrichten.

Anpassen

Farbschema

System > Anpassen > Farbschema

Die Seite **Farbschema** legt die Farben fest, die von der VSA-Umgebung für den aktuellen Benutzer angezeigt werden. Die Auswahl des **Farbschemas** gilt für alle Benutzer in derselben **Partition** *(siehe 631)*.

So ändern Sie das Farbschema:

1. Wählen Sie im mittleren Fensterbereich ein Farbschema aus.
2. Klicken Sie auf die Schaltfläche **Schema konfigurieren**.

Seitenanpassung

System > Anpassen > Seitenanpassung

Auf der Seite **Seitenanpassung** stehen folgende Registerkarten zur Anpassung der Benutzeroberfläche *für alle Benutzer* zur Verfügung.

- **Anmeldeseite** *(siehe 448)*

- **Website-Kopfzeile** *(siehe 448)*
- **Agent-Symbole** *(siehe 449)*
- **Kopfzeile einrichten** *(siehe 450)*
- **Titel des benutzerspezifischen Org-Feldes** *(siehe 450)*

Jede Registerkarte wird separat bearbeitet.

Anmeldeseite

System > Anpassen > Seitenanpassung > Anmeldeseite

Auf der Registerkarte **Anmeldeseite** der Seite **Seitenanpassung** werden die Optionen festgelegt, die bei einer Benutzeranmeldung angezeigt werden.

> **Hinweis:** Eine Zusammenfassung der Funktionen, die sich auf Benutzeranmeldungen auswirken, finden Sie unter **Anmelderichtlinien für VSA** *(siehe 401)*.

1. Klicken Sie auf der Registerkarte **Anmeldeseite** auf die Schaltfläche **Bearbeiten**. Das Dialogfeld **Anmeldeseite bearbeiten** wird angezeigt.
2. Die folgenden Einstellungen sind optional:
   - **Logo für die Anmeldeseite** – Blättern Sie zu einem benutzerdefinierten Logo auf Ihrem lokalen Rechner oder Netzwerk.

     > **Hinweis:** Ihr Logo sollte die empfohlene Größe nicht überschreiten.

   - **Titel** – Geben Sie Titeltext für diese Umgebung ein. Der Titel wird gleich unter dem Logo auf der Anmeldeseite angezeigt.
   - **Rechter-Frame-URL** – Geben Sie den Pfad einer benutzerdefinierten Webseite ein. Dieser Pfad muss relativ zum Verzeichnis `Webpages` oder `Webpages\Access` bzw. eine vollständig geformte URL sein.
   - **Systemversion auf der Anmeldeseite anzeigen** – Wenn dies aktiviert ist, wird die Systemversion angezeigt.
   - **'Passwort vergessen?' auf Anmeldeseite anzeigen** – Wenn dies aktiviert ist, wird der Hyperlink **Passwort vergessen?** auf der Anmeldeseite angezeigt. Wenn Sie auf den Link **Passwort vergessen?** auf der Anmeldeseite klicken (falls dies über die Registerkarte "System > Seitenanpassung > **Anmeldeseite** *(siehe 448)*" aktiviert wurde), wird Ihnen per E-Mail ein Link zum Ändern Ihres Passworts gesendet. Zum Ändern des Passworts müssen Sie bereits eine **Sicherheitsfrage** und **Sicherheitsantwort** festgelegt haben, und zwar über "System > **Login ändern** *(siehe 404)*".
   - **Systemstatus auf der Anmeldeseite anzeigen** – Wenn dies aktiviert ist, wird der Systemstatus auf der Anmeldeseite angezeigt.
   - **Kunden-ID auf der Anmeldeseite anzeigen** – Wenn dies aktiviert ist, wird die Kunden-ID auf der Anmeldeseite angezeigt.

Website-Kopfzeile

System > Anpassen > Seitenanpassung > Website-Kopfzeile

1. Klicken Sie auf der Registerkarte **Seitenkopfzeile** auf die Schaltfläche **Bearbeiten**. Das Dialogfeld **Seitenkopfzeile bearbeiten** wird angezeigt.
2. Die folgenden Einstellungen können angepasst werden:
   - **Logo** – Blättern Sie zu einem benutzerdefinierten Logo auf Ihrem lokalen Rechner oder Netzwerk. Klicken Sie auf die Schaltfläche **Standard**, um die Standardwerte wiederherzustellen.

> **Hinweis:** Standardmäßig zeigen VSA-Berichtskopfzeilen das unter "System > Seitenanpassung > **Website-Kopfzeile** *(siehe 448)*" angegebene Bild an. Durch Änderung des Werts in "System > Konfigurieren > **Berichtskonfiguration ändern** *(siehe 434)* > **Logo**" können Sie diese Standardeinstellung überschreiben und die URL *nur für Berichtskopfzeilen ändern*. Die Änderung der URL im Feld "Berichtskonfiguration ändern > **Logo**" wirkt sich nicht auf das Bild in der **Website-Kopfzeile** aus.

- **Titel** – Geben Sie einen benutzerdefinierten Titel ein, der neben dem Logo angezeigt wird. Klicken Sie auf die Schaltfläche **Standard**, um die Standardwerte wiederherzustellen.
- **Höhe der Kopfzeile** – Die Höhe der Kopfzeile in Pixeln. Die Standardeinstellung ist 50.
- **Symbol "Favoriten"** – Wenn für Ihre VSA-Website in einem Browser ein Lesezeichen gesetzt wird, wird neben dem Lesezeichentext dieses Symbol angezeigt. Sie können dafür ein beliebiges ICO-Bild der Größe 16 x 16 Pixel verwenden.

> **Hinweis:** Das **Symbol "Favoriten"** wird im **SaaS** *(siehe 631)*-basierten VSA nicht unterstützt.

Agent-Symbole

System > Anpassen > Seitenanpassung > Agent-Symbole

1. Klicken Sie auf der Registerkarte **Agent-Symbole** auf die Schaltfläche **Bearbeiten**. Das Dialogfeld **Agent-Symbole bearbeiten** wird angezeigt.
2. Laden Sie benutzerdefinierte Windows-Symbole auf den Kaseya Server hoch. Windows-Symbole müssen im .ico-Format vorliegen und die Farbtiefe darf 256 Farben nicht überschreiten. Die empfohlene Höchstgröße beträgt 32 x 32 Pixel.
   - **Agent online** – Der Agent checkt erfolgreich ein.
   - **Agent offline** – Der Agent checkt nicht ein.
   - **Agent blinkt** – Eine Nachricht wartet darauf, vom Rechnerbenutzer gelesen zu werden.
   - **Fernsteuerung ist deaktiviert** – Die Fernsteuerung des verwalteten Rechners wurde vom Rechnerbenutzer deaktiviert.
3. Laden Sie benutzerdefinierte Mac-Symbole auf den Kaseya Server hoch. Mac-Symbole müssen im .tif-Format vorliegen und die Farbtiefe darf 32 Bit nicht überschreiten. Die empfohlene Höchstgröße beträgt 48 x 48 Pixel.
   - **Agent online** – Der Agent checkt erfolgreich ein.
   - **Agent offline** – Der Agent checkt nicht ein.
   - **Agent blinkt** – Eine Nachricht wartet darauf, vom Rechnerbenutzer gelesen zu werden.
   - **Fernsteuerung ist deaktiviert** – Die Fernsteuerung des verwalteten Rechners wurde vom Rechnerbenutzer deaktiviert.

   > **Hinweis:** Benutzerdefinierte Mac-Symbolbilder erscheinen zwar nicht auf der Seite **Seitenanpassung**, werden aber korrekt angezeigt, wenn nachfolgend ein Agent-Installationspaket erstellt und auf einem Mac-Rechner installiert wird.

4. Laden Sie benutzerdefinierte Linux-Symbole auf den Kaseya Server hoch. Linux-Symbole müssen im .png-Format vorliegen und die Farbtiefe darf 256 Farben nicht überschreiten. Die empfohlene Höchstgröße beträgt 24 x 24 Pixel.
   - **Agent online** – Der Agent checkt erfolgreich ein.
   - **Agent offline** – Der Agent checkt nicht ein.
   - **Agent blinkt** – Eine Nachricht wartet darauf, vom Rechnerbenutzer gelesen zu werden.
   - **Fernsteuerung ist deaktiviert** – Die Fernsteuerung des verwalteten Rechners wurde vom Rechnerbenutzer deaktiviert.

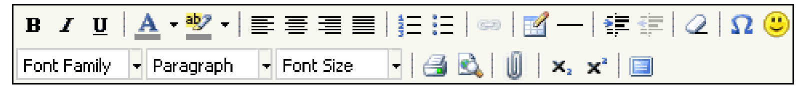
Hinweis: Weitere Informationen erhalten Sie unter **Benutzerdefinierte Agent-Symbole erstellen** *(siehe 450)*.

Kopfzeile einrichten

System > Anpassen > Seitenanpassung > Kopfzeile einrichten

Passen Sie das Logo und den Text an, die dem Benutzer angezeigt werden, wenn er über "Agent > **Agent bereitstellen** *(siehe 40)*" eine Webseite öffnet, um ihn zum Installieren des Agents aufzufordern.

Verwenden Sie die Werkzeugleiste, um dem Text Bilder oder eine spezielle Formatierung hinzuzufügen. *Bilder müssen hochgeladen und können nicht einfach kopiert und eingefügt werden.*



- – Hyperlink für ausgewählten Text. Möglicherweise müssen Sie Links, die von einer anderen Quelle eingefügt wurden, zurücksetzen.
- – Tabelle einfügen
- — – Horizontale Linie als einen Prozentsatz der Breite einfügen oder eine feste Breite in Pixel festlegen
- – Text einrücken
- – Text ausrücken
- – Formatierung entfernen
- Ω – Symbol einfügen
- – Emoticon einfügen
- – Bild- und Textvorschau anzeigen
- – Datei oder Bild hochladen
- x_2 – Ausgewählten Text tiefgestellt festlegen
- x^2 – Ausgewählten Text hochgestellt festlegen
- – Vollbildmodus zur Ansicht und Bearbeitung ein- und ausschalten

Titel des benutzerspezifischen Org-Feldes

System > Anpassen > Seitenanpassung > Titel des benutzerspezifischen Org-Feldes

Hier passen Sie die Namen der benutzerdefinierten Felder an, mit denen Organisationen klassifiziert werden. Die Werte der benutzerdefinierten Felder weisen Sie unter "System > Orgn./Gruppen/Abtlg./Personal > Verwalten > **Benutzerdefinierte Felder** *(siehe 427)* zu.

Benutzerdefinierte Agent-Symbole erstellen

Vier Agent-Symbole

Erstellen Sie *vier Symbole*, um benutzerdefinierte Agent-Symbole in die Systemablage (Windows) oder Menüleiste (Mac OS X) jedes verwalteten Rechners einzufügen. Diese Symbole müssen benannt werden:

Bei Windows-Agents

- `online.ico` – Standardmäßig ist dies das blaue K-Symbol , das angezeigt wird, wenn ein Agent mit dem Kaseya Server verbunden ist.
- `offline.ico` – Standardmäßig ist dies das graue K-Symbol, das angezeigt wird, wenn ein Agent nicht mit dem Kaseya Server verbunden ist.

- `blink.ico` – Standardmäßig ist dies das weiße K-Symbol, das angezeigt wird, wenn der Agent erfordert, dass der Benutzer auf das Symbol klickt, um eine Meldung anzuzeigen.
- `noremote.ico` – Standardmäßig ist dies das rote K-Symbol, das angezeigt wird, wenn der Benutzer das Menüelement **Remote Control deaktivieren** aus dem Agent-Popup-Menü ausgewählt hat.

Bei Mac-Agents

- `macOnline.tif` – Standardmäßig ist dies das blaue K-Symbol, das angezeigt wird, wenn ein Agent mit dem Kaseya Server verbunden ist.
- `macOffline.tif` – Standardmäßig ist dies das graue K-Symbol, das angezeigt wird, wenn ein Agent nicht mit dem Kaseya Server verbunden ist.
- `macNoremote.tif` – Standardmäßig ist dies das weiße K-Symbol, das angezeigt wird, wenn der Agent erfordert, dass der Benutzer auf das Symbol klickt, um eine Meldung anzuzeigen.
- `macBlink.tif` – Standardmäßig ist dies das rote K-Symbol, das angezeigt wird, wenn der Benutzer das Menüelement **Remote Control deaktivieren** aus dem Agent-Popup-Menü ausgewählt hat.

Bei Linux-Agents

- `linuxOnline.png` – Standardmäßig ist dies das blaue K-Symbol, das angezeigt wird, wenn ein Agent mit dem Kaseya Server verbunden ist.
- `linuxOffline.png` – Standardmäßig ist dies das graue K-Symbol, das angezeigt wird, wenn ein Agent nicht mit dem Kaseya Server verbunden ist.
- `linuxNoremote.png` – Standardmäßig ist dies das weiße K-Symbol, das angezeigt wird, wenn der Agent erfordert, dass der Benutzer auf das Symbol klickt, um eine Meldung anzuzeigen.
- `linuxBlink.png` – Standardmäßig ist dies das rote K-Symbol, das angezeigt wird, wenn der Benutzer das Menüelement **Remote Control deaktivieren** aus dem Agent-Popup-Menü ausgewählt hat.

Benutzerdefinierte Agent-Symbole formatieren

Bei benutzerdefinierten **Windows**-Symbolen:

- Das Format muss das Windows-Symbolformat verwenden. Eine einfache Bitmap-Datei kann nicht einfach mit der Erweiterung .ico umbenannt werden.
- Die empfohlene Höchstgröße beträgt 32 x 32 Pixel.
- Die Farbtiefe darf 8-Bit-Farbe (256 Farben) nicht überschreiten.

Bei benutzerdefinierten Agent-Symbolen auf **Apple**:

- Das Format muss .tif sein.
- Die empfohlene Höchstgröße beträgt 48 x 48 Pixel.
- Die Farbtiefe sollte RGB-32-Bit sein.

Bei benutzerdefinierten Agent-Symbolen auf **Linux**:

- Das Format muss .png sein.
- Die empfohlene Höchstgröße beträgt 24 x 24 Pixel.
- Die Farbtiefe darf 8-Bit-Farbe (256 Farben) nicht überschreiten.

Benutzerdefinierte Symbole installieren

1. Gehen Sie zur Registerkarte "System > Seitenanpassung > **Agent-Symbole** *(siehe 449)*".
2. Klicken Sie auf die Registerkarte **Agent-Symbole**.
3. Klicken Sie auf die Schaltfläche **Bearbeiten**. Das Dialogfeld **Agent-Symbole bearbeiten** wird angezeigt.
4. Klicken Sie auf die Schaltfläche 'Durchsuchen' für ein beliebiges Agent-Symbol, um ein benutzerdefiniertes Agent-Symbol auf Ihrem lokalen Rechner auszuwählen.

5. Klicken Sie wahlweise auf die Schaltflächen **Standard verwenden**, um die Agent-Symbole auf ihre Standardbilder zurückzusetzen.

Vorhandene Agents mit benutzerdefinierten Agent-Symbolen aktualisieren

Die benutzerdefinierten Agent-Symbole werden automatisch bereitgestellt, wenn Agents über die Registerkarte "Agent > **Agent aktualisieren** *(siehe 81)*" aktualisiert werden. Sie müssen das Kontrollkästchen **Update erzwingen** aktivieren, um Agents der aktuellen Version zu aktualisieren.

Agent-Installationspakete mit benutzerdefinierten Agent-Symbolen erstellen

Aktualisierte Agent-Symbole sind in allen neu heruntergeladenen `KcsSetup`-Dateien enthalten, die über **Agent verteilen** *(siehe 40)* erstellt werden. Wenn Sie eine `KcsSetup`-Datei eines Agent-Installationsprogramms in ein Domänen-Anmeldeskript eingefügt haben, müssen Sie die `KcsSetup`-Datei erneut herunterladen, damit die aktualisierten Symbole berücksichtigt werden und die Datei auf dem Domänenserver ersetzt wird.

Lokale Einstellungen

System > Anpassen > Lokale Einstellungen

Ab dieser Version werden die folgenden Einstellungen systemweit angewendet. Diese Einstellungen betreffen derzeit die Module **Zeitüberwachung** und **Service Billing**.

Datumsformat

- **Format** – Bestimmt das Datumsformat im VSA.
  - MM/TT/JJJJ
  - TT/MM/JJJJ
  - JJ/MM/TT
- **Trennzeichen** – Bestimmt das Trennzeichen für das Datumsformat im VSA.
  - / (Schrägstrich)
  - - (Bindestrich)
  - . (Punkt)

> **Hinweis:** Das Zeitformat wird unter "System > **Konfigurieren** *(siehe 429)*" eingestellt.

Zahlenformat

- **Dezimalstellen** – Legt die Anzahl der Dezimalstellen für die Währungsanzeige im VSA fest. Bis zu 3 Dezimalstellen sind möglich.
- **Dezimalformat** – Legt das Dezimalformat für die Währungsanzeige im VSA fest.
  - xx,xxx.xx
  - xx.xxx,xx

Anpassen: Live-Connect

System > Anpassen > Live-Connect

Auf der Seite **Anpassen: Live Connect** werden die in den Fenstern **Live Connect** *(siehe 393)* und **Portalzugriff** *(siehe 75)* angezeigten Registerkarten für die **Startseite** angepasst. Sie können mehrere angepasste Registerkarten für **Startseite** erstellen und nach Namen speichern.

Diese Registerkarten der **Startseite** werden für eine bestimmte Rolle aktiviert, indem Sie das Kontrollkästchen unter "Live-Connect > Startseite" aktivieren, und zwar in:

- System > Benutzerrollen > **Zugriffsrechte** *(siehe 415)*
- System > Rechnerrollen > **Zugriffsrechte** *(siehe 418)*

> **Hinweis:** Im ersten Thema der Online-Hilfe können Sie eine PDF-Datei zu Live-Connect herunterladen.

Sie können drei Abschnitte auf der standardmäßigen **Startseite** anpassen.

- **Portal-Kopfzeile** – Passen Sie den Text und das Bild an, der/das oben auf der Registerkarte **Startseite** angezeigt wird.
- **Agent-Verfahren** – Stellen Sie eine benutzerdefinierte Liste von Agent-Verfahren bereit, die der Benutzer sofort über diese Registerkarte ausführen kann.
- **Benutzerdefinierte Links** – Stellen Sie eine benutzerdefinierte Liste von URLs bereit, auf die der Benutzer auf dieser Registerkarte klicken kann. Beispielsweise könnten Sie eine URL zu einer Webseite bereitstellen, die technische Informationen über die Fehlerbehebung auf verwalteten Rechnern liefert.

Allen Tenants zur Verfügung stellen

Wenn dies aktiviert ist, kann die Startseite zu Benutzerrollen und Rechnerrollen in allen Tenant-Partitionen hinzugefügt werden. Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt.

Kapitel 10

Ticketing

In diesem Kapitel

Ticketing – Überblick

Über das **Ticketing**-Modul werden Serviceanfragen verwaltet. Diese Serviceanfragen und Ihre Antworten darauf werden anhand von **Tickets** dokumentiert.

Das Ticketing-System benachrichtigt die designierten VSA-Benutzer und Ticket-Absender automatisch per E-Mail bei Systemereignissen wie beispielsweise der Erstellung, Änderung oder Auflösung von Tickets. Das System organisiert Tickets nach Rechner-ID, Gruppen-ID, Organisations-ID, Abteilungs-ID oder Mitarbeiter-ID. Sie können eine "generische" Organisation unter "System > **Verwalten** *(siehe 423)*" erstellen, in der globale Tickets wie beispielsweise allgemeine Netzwerkprobleme gehalten werden.

Sichtbarkeit von Tickets in anderen Modulen

Tickets können auch mit **Live-Connect** *(siehe 393)* und unter "Infocenter > **Dashboard anzeigen** *(siehe 241)*" angezeigt werden.

Funktionen	Beschreibung
Übersicht anzeigen *(siehe 457)*	Listet alle Tickets auf. Auf jeder Zeile werden Übersichtsdaten für ein einzelnes Ticket angezeigt.
Erstellen/Anzeigen *(siehe 460)*	Erstellen Sie neue Tickets oder fügen Sie Anmerkungen zu bestehenden Tickets hinzu bzw. ändern Sie diese.
Löschen/Archivieren *(siehe 463)*	Löschen Sie Tickets permanent oder verschieben Sie sie in einen Archivspeicher.
Tickets migrieren *(siehe 465)*	Migrieren Sie Tickets aus Ticketing zu **Service Desk**-Tickets und umgekehrt.
Benachrichtigungsrichtlinie *(siehe 466)*	Legen Sie fest, wann E-Mail-Benachrichtigungen vom Ticketing-Modul versendet werden.
Zugriffsrichtlinie *(siehe 467)*	Legen Sie fest, wer Felder in Tickets bearbeiten und/oder anzeigen kann.
Richtlinie über Bearbeiterzuordnung *(siehe 469)*	Erstellen Sie Regeln, um Benutzer automatisch einem neuen oder bestehenden Ticket zuzuweisen.
Fälligkeitsrichtlinie *(siehe 469)*	Definieren Sie standardmäßige Fälligkeitsdaten für neue Tickets basierend auf Feldwerten und den Betreff-Zeilen von E-Mails.
Felder bearbeiten *(siehe 471)*	Definieren, ändern oder erstellen Sie Ticketfelder, die zur Klassifizierung von Tickets dienen.
E-Mail-Leseprogramm *(siehe 472)*	Richten Sie automatisches Polling eines POP3-E-Mail-Servers ein, um neue Ticket-Einträge zu generieren.
E-Mail-Mapping *(siehe 474)*	Definieren Sie die Standard-Feldwerte für neue Tickets, die mit dem E-Mail-Leseprogramm erhalten werden.

Übersicht anzeigen

Ticketing > Tickets verwalten > Übersicht anzeigen

- Ähnliche Informationen werden auch unter "Infocenter > Reporting > Berichte > Ticketing *(siehe 239)*" angezeigt.

Auf der Seite **Übersicht anzeigen** werden alle Tickets aufgelistet. Auf jeder Zeile werden Übersichtsdaten für ein einzelnes Ticket angezeigt.

Neue Tickets oder Neue Anmerkungen

Neue Tickets order neue Anmerkungen in bestehenden Tickets werden auf eine von zwei Arten markiert.

- **Nach Datum** – Tickets mit neuen Anmerkungen, die innerhalb des letzten Tages eingegeben wurden, sind rot markiert. Neue Anmerkungen, die in den letzten 7 Tagen eingegeben wurden, sind gelb markiert. Sie können diese Zeiten und Farben durch Klicken auf den Link **Markierung ändern** anpassen.
- **Lesen-Marker** – Jedes Ticket wird markiert, um anzudeuten, ob der Benutzer alle Anmerkungen in dem Ticket angezeigt hat. Nachdem ein Ticket angezeigt wurde, wird es mit dem Symbol als gelesen markiert. Wenn ein anderer Benutzer oder der ursprüngliche Benutzer eine Anmerkung hinzufügt oder ändert, wird das Ticket wieder mithilfe des Symbols als ungelesen markiert.

Filtern

Die Liste der angezeigten Tickets ist von verschiedenen Faktoren abhängig:

- Die Liste der angezeigten Rechner basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem **Scope** *(siehe 419)* des Benutzers.
- Sie können die aufgelisteten Tickets weiter *sortieren* und *filtern*, indem Sie in den Dropdown-Listen des Feldes Werte auswählen.
- Bei einer **Suche** werden keine Tickets angezeigt, wenn die Tickets keines der Wörter enthalten, nach denen gesucht wird.
- Die Benutzer eines Rechners haben über **Portalzugriff** *(siehe 75)* nur Zugriff auf die Tickets für ihre eigene Rechner-ID.

Administratoren

Die mit **Übersicht anzeigen** *(siehe 457)* und **Erstellen/Anzeigen** *(siehe 460)* angezeigte Administratorenliste basiert auf dem Umfang des gegenwärtig angemeldeten Benutzers. Über die Ticketzuweisung im **Ticketing**-Modul können Sie unabhängig von Ihrer Rolle oder Ihrem Umfang stets die Haupt-Benutzer anzeigen.

Tickets öffnen, Überfällig, Geschlossene Tickets, Gesamte Tickets

Zeigt die Anzahl der offenen, geschlossenen und überfälligen Tickets und der Tickets insgesamt für alle Tickets, die die oben beschriebenen Filterkriterien erfüllen.

Suchen

Suchen schränkt die Liste der Tickets auf diejenigen Tickets ein, die **eines** der Wörter oder Ausdrücke in der Suchzeichenfolge enthalten. Schließen Sie Ausdrücke in doppelte Anführungszeichen (") ein. Bei einer Suche werden die **Übersicht**szeile des Tickets, der **Name**, die **E-Mail**-Adresse und die **Telefonnummer** des Absenders und sämtliche **Anmerkungen** geprüft.

> **Hinweis:** Ein Sternchen (*) im Suchfeld findet nur Tickets mit einem Sternchen.

Beim Klicken auf einen der **Übersichts**-Links des Tickets im Seitenbereich werden die Details dieses

Tickets auf der Seite **Ticket anzeigen** *(siehe 460)* eingeblendet. Wörter in den Ticket-Anmerkungen, die mit einem der **Such**begriffe übereinstimmen, werden *mit einem grünen Hintergrund hervorgehoben.*

<Letzte 10 Suchen>

In der Dropdown-Liste unterhalb des Bearbeitungsfelds **Suchen** werden Ihre `<last 10 searches>` aufgeführt. Wenn Sie ein Element aus dieser Liste auswählen, wird automatisch erneut nach diesen Wörtern gesucht.

Sortieren

Klicken Sie auf **aufsteigend** oder **absteigend**, um die Tickets in der ausgewählten Spalte zu sortieren.

Felder...

Mit dieser Option kann jeder Benutzer die in der Tabelle angezeigten Spalten organisieren. Durch Klicken auf **Felder...** wird ein Dialogfeld in einem neuen Browser-Fenster geöffnet. Hier können Sie auswählen, welche Spalten ein- oder ausgeblendet werden und ihre Reihenfolge festlegen. Beliebige der folgenden Spalten können ein- oder ausgeblendet werden:

- **ID** – Eindeutige ID, die automatisch jedem Ticket zugewiesen wird.
- **Rechner-ID** – Das auf diesen Rechner angewendete Ticket.
- **Administrator** – Der Name des für die Lösung des Problems zuständigen Benutzers.
- **Kategorie** – Art des Problems, auf das in diesem Ticket eingegangen wird.
- **Status** – Offen, Warteliste, Geschlossen
- **Priorität** – Hoch, Normal, Niedrig
- **SLA-Typ** – Art des Service-Level-Agreements
- **Tech. senden** – Ja, Nein
- **Bestätigung** – Erforderlich, Nicht erforderlich
- **Arbeitsstunden** – Arbeitsstunden im Dezimalformat.
- **Letztes Änderungsdatum** – Zeitpunkt, zu dem zuletzt eine Anmerkung zu diesem Ticket hinzugefügt wurde.
- **Erstellungsdatum** – Zeitpunkt, zu dem das Ticket erstmals eingegeben wurde.
- **Fälligkeitsdatum** – Fälligkeitsdatum des Tickets.
- **Auflösungsdatum** – Datum, an dem das Ticket geschlossen wurde.
- **Absendername** – Person, die das Ticket eingesendet hat: Benutzer, Benutzername oder Rechner-ID.
- **Absender-E-Mail** – E-Mail-Adresse des Absenders.
- **Absender-Telefon** – Telefonnummer des Absenders.

Sie können auch weitere benutzerdefinierte Felder auswählen, die Sie zuvor mit "Ticketing > **Felder bearbeiten** *(siehe 471)*" erstellt haben.

Bei Feldänderungen automatisch einreichen/Einreichen

Wenn **Bei Feldänderungen automatisch einreichen** aktiviert ist, wird die Seite **Übersicht anzeigen** erneut angezeigt, wann immer ein Feld im **Listenfeld-Filter** geändert wird. Wenn diese Option nicht aktiviert ist, können Sie mehrere **Listenfeld-Filter** gleichzeitig ändern. Die Seite **Übersicht anzeigen** wird erst dann wieder angezeigt, wenn Sie auf **Einreichen** klicken.

(Listenfeld-Filter)

Jedes Feld des Typs `List`, wie beispielsweise **Kategorie**, **Status** oder **Priorität**, wird auch als auswählbare Dropdown-Liste angezeigt. Wenn Sie Werte aus einer oder mehreren dieser Dropdown-Listen auswählen, wird der Seitenbereich gefiltert, sodass nur die Tickets angezeigt werden, die den ausgewählten Werten entsprechen. Benutzerdefinierte `List`-Felder werden unter "Ticketing > **Felder bearbeiten** *(siehe 471)*" erstellt.

Alle gelesenen markieren

Klicken Sie, um alle Tickets als gelesen zu markieren Für gelesene Tickets wird ein Symbol angezeigt. Bei Änderungen oder Anmerkungsergänzungen, die von anderen Benutzern eingefügt werden, wird das Ticket wieder auf ungelesen zurückgesetzt. Für ungelesene Tickets wird ein Symbol angezeigt.

Feld festlegen...

Mit **Feld einstellen...** können Sie mehrere Feldwerte auf mehreren Tickets gleichzeitig ändern. Markieren Sie dieses Feld für alle Tickets, für die Sie einen Feldwert ändern wollen. Klicken Sie anschließend auf **Feld einstellen...** Ein Dialogfeld wird angezeigt, über das Sie einen neuen Wert für beliebige der Felder festlegen können.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Zusammenführen...

Um Tickets zusammenzuführen, *markieren Sie das Feld für zwei beliebige aufgelistete Tickets* und klicken Sie dann auf **Zusammenführen...**. Das resultierende zusammengeführte Ticket enthält alle Anmerkungen und Anhänge von beiden Tickets. Sie werden gefragt, welche Feldwerte Sie in dem Ticket für alle Feldwerte verwenden möchten, die in den beiden Tickets verschieden sind.

Markierung ändern

Klicken Sie auf **Markierung ändern**, um die Zeilenmarkierung basierend auf dem Datum einzustellen und/oder zu ändern. Sie können Tickets auf zweierlei Weisen markieren. Tickets mit einem Datum innerhalb von 1 Tag der aktuellen Uhrzeit sind rot markiert. Tickets mit einem Datum innerhalb von 7 Tagen sind gelb markiert. Sie können nach freiem Ermessen *die Anzahl der Tage und die Markierungsfarbe anpassen*. Um die Markierung nach Datum zu deaktivieren, setzen Sie die Anzahl der Tage für alle Tickets auf Null. Als Markierungsdatum kann das **letzte Änderungsdatum**, das **Fälligkeitsdatum** oder das **Erstellungsdatum** dienen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Spaltenüberschriften

Durch Klicken auf eine Spaltenüberschrift wird die Tabelle unter Verwendung dieser Spalte als Sortierkriterium neu geordnet.

Datentabelle

Auf jeder Zeile der Tabelle werden Übersichtsdaten für ein einzelnes Ticket angezeigt.

- Um die Details des Tickets in einem *neuen Fenster* anzuzeigen, klicken Sie auf das Symbol für ein neues Fenster . Wenn Sie den Mauszeiger über das Symbol eines Tickets halten, wird ein Vorschaufenster der aktuellen Anmerkungen für dieses Ticket angezeigt. Darin können Sie die Tickets in Ihrer Warteschlange schnell überprüfen. Die Anzahl der Millisekunden, die der Cursor sich über einem Symbol befinden muss, kann unter "System > **Voreinstellungen** *(siehe 402)*" festgelegt werden.
- Um die Details des Tickets im *gleichen Fenster* anzuzeigen, klicken Sie auf den Link für die **Übersicht**szeile.
- Um den Status zu *Gelesen* zu ändern, klicken Sie auf .
- Um den Status zu *Nicht gelesen* zu ändern, klicken Sie auf .

Erstellen/Anzeigen

Ticketing > Tickets verwalten > Erstellen/Anzeigen

Auf der Seite **Erstellen/Anzeigen** erstellen Sie neue Tickets oder fügen Sie Anmerkungen zu bestehenden Tickets hinzu bzw. ändern sie.

Neues Ticket hinzufügen

1. Umgehen Sie das Feld **Ticket-ID**. In dieses Feld wird beim Erstellen des Tickets eine neue eindeutige Zahl eingetragen.
2. Klicken Sie auf **Verknüpfung auswählen**, um das Ticket mit einem von sechs Typen von VSA-Datensätzen zu verknüpfen: Bestand, Rechner-ID, Rechnergruppe, Organisation, Abteilung oder Mitarbeiter. Dieser Schritt ist obligatorisch.
3. Geben Sie eine kurze Beschreibung des Problems in das Feld **Übersicht** ein.
4. In die Felder der Ticket-**Absender** werden die folgenden Werte eingetragen:
   - Falls in Schritt 2 eine Rechner-ID ausgewählt wurde, werden in die Felder **Benutzername**, **Benutzer-E-Mail** und **Benutzer-Telefonnummer** des Ticket-Absenders die Kontaktdaten eingegeben, die für diese Rechner-ID unter "Agent > **Profil bearbeiten** *(siehe 73)*" gespeichert sind. Diese Informationen können nach Bedarf aktualisiert werden.
   - Falls in Schritt 2 eine andere Angabe außer Rechner-ID ausgewählt wurde, können diese Felder des Ticket-Absenders nach Bedarf manuell ausgefüllt werden.
   - Wurde ein Ticket über "Ticketing > **E-Mail-Leseprogramm** *(siehe 472)*" durch eine eingehende E-Mail-Nachricht erstellt, wird in das Feld **Absender-E-Mail** die E-Mail-Adresse des Absenders eingetragen.
5. Das **Erstellungsdatum** wird automatisch zugewiesen.
6. Das Datum für **Alter/Geschlossen** wird automatisch zugewiesen. Unter **Alter** wird für nicht geschlossene Tickets die Anzahl der Stunden/Tage seit dem Erstellungsdatum aufgelistet. Wurde das Ticket bereits geschlossen, wird **Alter** durch **Geschlossen** ersetzt, und es wird das Datum und die Uhrzeit, zu der dieses Ticket geschlossen wurde, angezeigt.
7. Das Standard-Fälligkeitsdatum eines Tickets wird mit "Ticketing > **Fälligkeitsrichtlinie** *(siehe 469)*" bestimmt. Das Fälligkeitsdatum ergibt sich aus den Ticketattributen, die beim Eingeben eines *neuen* Tickets angegeben wurden. Falls für ein Ticket eine Fälligkeitsregel gilt, wird neben dem Fälligkeitsdatum ein Regelsymbol angezeigt. Sie können das bestehende Fälligkeitsdatum überschreiben, indem Sie auf das Bearbeitungssymbol neben dem Fälligkeitsdatum klicken. Das Regelsymbol wird durch ein Symbol für manuelles Überschreiben neben dem Fälligkeitsdatum ersetzt. Klicken Sie auf **Anwenden**, um das Fälligkeitsdatum auf das durch die Regel festgelegte Fälligkeitsdatum zurückzusetzen. Falls das Fälligkeitsdatum keiner der definierten **Fälligkeitsregeln** *(siehe 469)* entspricht, wird die Bezeichnung **Fälligkeitsdatum** markiert. Falls keine Fälligkeitsregeln definiert sind, wird das Standard-Fälligkeitsdatum des Systems verwendet. Dieses ist auf eine Woche nach dem Erstellungsdatum des Tickets gesetzt. Wenn ein Ticket überfällig ist, wird das Fälligkeitsdatum als fettgedruckter dunkelroter Text auf der Seite **Übersicht anzeigen** *(siehe 457)* und in **Ticketing** *(siehe 239)*-Berichten angezeigt. Es wird außerdem als roter Text in der Kopfzeile der Seite **Erstellen/Anzeigen** *(siehe 460)* angezeigt. Sie können unter "Ticketing > **Benachrichtigungsrichtlinie** *(siehe 466)*" wahlweise eine E-Mail für überfällige Tickets senden. Ein Ticket gilt als aufgelöst, wenn sein Status auf 'Geschlossen' eingestellt und das Auflösungsdatum aufgezeichnet wird.
8. Klassifizieren Sie das Ticket mithilfe der integrierten Felder des Typs `List`, wie beispielsweise **Bearbeiter**, **Kategorie**, **Status** oder **Priorität**. Sie können das Ticket auch unter Verwendung weiterer Felder des Typs `List` klassifizieren, die unter "Ticketing > **Felder bearbeiten** *(siehe 471)*" für Tickets erstellt wurden.
9. Geben Sie Details des Problems in das Bearbeitungsfeld **Anmerkungen** ein. Klicken Sie auf den Link **Anmerkungsgröße**, um die Anzahl der Zeilen für Ihren Anmerkungstext zu ändern.

10. Um eine Datei, wie beispielsweise einen Screenshot an das Ticket anzuhängen, klicken Sie unterhalb des Anmerkungseingabebereichs auf **Blättern...**. Ermitteln Sie die anzuhängende Datei auf Ihrem lokalen Computer. Klicken Sie im Suchfenster auf **Öffnen**, um die Datei auf den VSA-Server hochzuladen. Sobald die Datei erfolgreich hochgeladen wurde, wird automatisch Tag-Text in die Anmerkung im folgenden Format eingegeben: `<attached file:filename.ext>`. Dieser Tag erscheint als Hyperlink in einer Anmerkung für das Ticket. Durch Klicken auf diesen Link können Sie die Datei jederzeit anzeigen/herunterladen.

> **Hinweis:** Die folgende Liste von Dateinamenerweiterungen wird in der Anmerkung als Grafiken oder Text anstelle eines mit Hyperlink versehenen Dateinamens angezeigt: gif, jpg, png, bmp, txt, sql.
>
> **Hinweis:** Ticket-Dateianhänge befinden sich für gewöhnlich im Verzeichnis `C:\Kaseya\WebPages\ManagedFiles`.

11. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung unterdrücken**, falls keine E-Mail-Empfänger (weder VSA-Benutzer noch Rechnerbenutzer) über das Ticket benachrichtigt werden sollen. In den meisten Fällen lassen Sie diese Angabe leer.
12. Aktivieren Sie das Kontrollkästchen **Automatische Anmerkungserstellung unterdrücken**, falls Anmerkungen nicht automatisch hinzugefügt werden sollen. Diese Option ist standardmäßig ausgeblendet. Mithilfe von **Zugriffsregel** *(siehe 467)* können Sie sie einblenden.
13. Die Erstellung des Tickets kann auf eine von zwei Weisen abgeschlossen werden:
    - Klicken Sie auf **Abschicken**, um die Ticketerstellung abzuschließen und VSA-Benutzer *und* Rechnerbenutzer per E-Mail zu benachrichtigen.
    - Klicken Sie auf **Neu ausgeblendet**, um die Ticketerstellung abzuschließen und *nur VSA-Benutzer* per E-Mail zu benachrichtigen. In ausgeblendeten Anmerkungen können Sie Daten oder Analysen aufzeichnen, die für Rechnerbenutzer zu detailliert oder verwirrend, für VSA-Benutzer jedoch hilfreich sein können.

> **Hinweis:** Ausgeblendete Anmerkungen werden *niemals* in E-Mail-Benachrichtigungen aufgenommen.

Vorhandenes Ticket bearbeiten

Um ein vorhandenes Ticket anzuzeigen, geben Sie eine Ticketnummer in das Feld **Ticket-ID** ein.

- Wenn Sie die Nummer des Tickets nicht kennen, ermitteln Sie dieses über **Übersicht anzeigen** *(siehe 457)* oder **Löschen/Archivieren** *(siehe 463)* und wählen das Ticket aus. Das Ticket wird auf dieser Seite angezeigt.
- Wenn ein vorhandenes Ticket erstmals auf dieser Seite angezeigt wird, zeigen die Kopfzeilenfelder die aktuellen Einstellungen für das Ticket.
- Wenn Sie an einem der Felder des Typs `Liste` Änderungen vornehmen, wird umgehend eine neue Anmerkung über die Änderung für das Ticket erstellt.
- Bei Änderungen an Feldern, die nicht vom Typ `Liste` sind, wie beispielsweise **Übersicht**, **Absenderinformationen** oder Felder, die Freiformtexteingaben oder Zahlen akzeptieren, müssen Sie anschließend auf **Aktualisieren** klicken, um eine neue Anmerkung zu erstellen.
- Bearbeiten Sie etwaige *frühere* Anmerkungen für ein Ticket, indem Sie auf das Bearbeiten-Symbol neben der zu bearbeitenden Anmerkung klicken. Daraufhin werden in die Kopfzeilenfelder die Einstellungen für diese Anmerkung eingetragen. Außerdem wird die Zeile in der Anmerkung, die Sie gerade bearbeiten, gelb markiert. Sie können den Inhalt der Anmerkung, einschließlich ihres Zeitstempels, ändern. Klicken Sie auf **Ändern**, um die vorgenommenen Änderungen zu bestätigen.
- Sie löschen die Anmerkung durch Klicken auf das nebenstehende Symbol Löschen.
- Durch Klicken auf das Symbol Trennen neben einer Anmerkung können Sie diese in zwei Tickets trennen. Das neue Ticket enthält diese Anmerkung und alle jüngeren Anmerkungen. Das ursprüngliche Ticket kann entweder geschlossen oder unverändert belassen werden.

> **Hinweis:** Die Berechtigungen zum Anzeigen, Bearbeiten und Löschen von Tickets und Feldern werden über "Ticketing > **Zugriffsrichtlinie** *(siehe 467)*" festgelegt. VSA-Benutzer und Rechnerbenutzer werden anhand der Einstellungen in "Ticketing > **Benachrichtigungsrichtliniesrichtlinie** *(siehe 466)*" über Ticketänderungen benachrichtigt. Ändern Sie die Nummer, die dem nächsten neuen Ticket automatisch zugewiesen wird, über **Felder bearbeiten** *(siehe 471)*.

Administratoren

Die mit **Übersicht anzeigen** *(siehe 457)* und **Erstellen/Anzeigen** *(siehe 460)* angezeigte Administratorenliste basiert auf dem Umfang des gegenwärtig angemeldeten Benutzers. Über die Ticketzuweisung im **Ticketing**-Modul können Sie unabhängig von Ihrer Rolle oder Ihrem Umfang stets die Haupt-Benutzer anzeigen.

Administratorregel-Symbol

Standardmäßig wird neben dem Bearbeiterfeld das Symbol für `always enforce assignee policy` angezeigt. Dieses weist darauf hin, dass die Administratornamen automatisch über **Administratorregel** *(siehe 469)* ausgewählt werden. Klicken Sie einmal auf das Symbol , um zum Symbol für `override the assignee policy` wechseln. Dadurch wird die Administratorregel überschrieben, und Sie können manuell einen Administrator auswählen.

> **Hinweis:** Falls für die Kombination der ausgewählten Werte in den Feldern des Typs `List` keine Richtlinie über die Bearbeiterzuordnung definiert ist, hat der Wechsel zwischen den Symbolen und keine Auswirkung.

Seite "Erstellen/Anzeigen" über eine URL anzeigen

Mit der folgenden URL wird die Webseite **Erstellen/Anzeigen** *(siehe 460)* für eine bestimmte Ticket-ID angezeigt.

```
http://...?ticid=<TicketID>
```

Zum Beispiel:

```
http://demo.kaseya.com?ticid=1234
```

Zeit/Admin

Listet die Zeit auf, zu der eine Änderung an einem Ticket vorgenommen wurde, und den Benutzer, der die Änderung vorgenommen hat.

Hinweis

Listet alle Anmerkungen zu diesem Ticket in auf- oder absteigender Reihenfolge nach Uhrzeit auf. Jede Anmerkung ist mit einem Zeitstempel und dem Anmeldenamen der Person, die die Anmerkung eingegeben hat, versehen.

> **Hinweis:** Von einem Benutzer eingegebene Anmerkungen werden mit der Rechner-ID gekennzeichnet, mit der sich der Benutzer angemeldet hat. Weitere Hinweise finden Sie unter **Portalzugriff** *(siehe 75)*.

Ausblenden

Falls diese Option aktiviert ist, wird diese Anmerkung für VSA-Benutzer ausgeblendet, für Rechnerbenutzer jedoch nicht. Die Standardeinstellung richtet sich nach dem Kontrollkästchen **Als ausgeblendete Anmerkung** unter "Ticketing > **Zugriffsrichtlinie** *(siehe 467)*". Zugriffsregeln werden abhängig von der Benutzerrolle zugewiesen. Falls Sie zu mehr als einer Benutzerrolle gehören, hat die restriktivste Regel Vorrang.

Löschen/Archivieren

Ticketing > Tickets verwalten > Löschen/Archivieren

Über die Seite **Löschen/Archivieren** können Sie alte Tickets oder Tickets in einer bestimmten Kategorie oder mit einem bestimmten Status löschen. Möglicherweise haben Sie einen Punkt erreicht, an dem Ihr System so viele alte Tickets aufweist, dass diese Ihre Suchvorgänge aufgrund veralteter Daten verlangsamen.

> **Hinweis:** Die Berechtigungen zum Anzeigen, Bearbeiten und Löschen von Tickets und Feldern werden unter "Ticketing > **Zugriffsrichtlinie** *(siehe 467)*" festgelegt.

Tickets archivieren

Sie können Tickets nicht nur löschen, sondern auch **archivieren**. Archivierte Tickets verbleiben in der Datenbank, werden jedoch in separate Tabellen verschoben. Mit der Funktion Archivieren können Sie überflüssige oder alte Tickets aus der aktiven Datenbank herausnehmen, **ohne** sie vom System zu löschen. Sie können Tickets jederzeit zwischen der aktiven und der Archiv-Datenbanktabelle hin und her verschieben.

Filtern

Die Liste der angezeigten Tickets ist von verschiedenen Faktoren abhängig:

- Die Liste der angezeigten Rechner basiert auf dem **Rechner-ID-/Gruppen-ID-Filter** *(siehe 26)* und dem **Scope** *(siehe 419)* des Benutzers.
- Sie können die aufgelisteten Tickets weiter *sortieren* und *filtern*, indem Sie in den Dropdown-Listen des Feldes Werte auswählen.
- Bei einer **Suche** werden keine Tickets angezeigt, wenn die Tickets keines der Wörter enthalten, nach denen gesucht wird.
- Die Benutzer eines Rechners haben über **Portalzugriff** *(siehe 75)* nur Zugriff auf die Tickets für ihre eigene Rechner-ID.
- Verwenden Sie die Steuerung **Tickets ausblenden, die zuletzt geändert wurden nach dem**, um nur diejenigen Tickets anzuzeigen, die *vor* einem bestimmten Datum erstellt oder geändert wurden.

Geschlossene Tickets archivieren

Führen Sie beispielsweise folgende Schritte aus, um Tickets mit dem Status `Closed` zu archivieren, die älter als 6 Monate sind:

1. Wählen Sie in **Status** den Eintrag `Geschlossen` aus.
2. Stellen Sie die Steuerung **Tickets ausblenden, die zuletzt geändert wurden nach dem** so ein, dass nur Tickets aufgelistet werden, die vor 6 Monaten oder länger geändert wurden.
3. Klicken Sie auf die Schaltfläche **Einstellen**.
4. Klicken Sie auf den Link **Alle auswählen**.
5. Klicken Sie auf die Schaltfläche **Archivieren...**.
6. Aktivieren Sie das Kontrollkästchen **Archivierte Tickets anstelle aktiver Tickets anzeigen**, um nach archivierten Tickets zu suchen und sie zu prüfen. Mit der Schaltfläche **Wiederherstellen...** können Sie Tickets wieder in die aktive Tabelle verschieben.

Tickets öffnen, Überfällig, Geschlossene Tickets, Gesamte Tickets

Zeigt die Anzahl der offenen, geschlossenen und überfälligen Tickets und der Tickets insgesamt für alle Tickets, die die oben beschriebenen Filterkriterien erfüllen.

Suchen

Suchen schränkt die Liste der Tickets auf diejenigen Tickets ein, die **eines** der Wörter oder Ausdrücke in der Suchzeichenfolge enthalten. Schließen Sie Ausdrücke in doppelte Anführungszeichen (") ein. Bei

einer Suche werden die **Übersicht**szeile des Tickets, der **Name**, die **E-Mail**-Adresse und die **Telefonnummer** des Absenders und sämtliche **Anmerkungen** geprüft.

> **Hinweis:** Ein Sternchen (*) im Suchfeld findet nur Tickets mit einem Sternchen.

Beim Klicken auf einen der **Übersichts**-Links des Tickets im Seitenbereich werden die Details dieses Tickets auf der Seite **Ticket anzeigen** *(siehe 460)* eingeblendet. Wörter in den Ticket-Anmerkungen, die mit einem der **Such**begriffe übereinstimmen, werden *mit einem grünen Hintergrund hervorgehoben.*

<Letzte 10 Suchen>

In der Dropdown-Liste unterhalb des Bearbeitungsfelds **Suchen** werden Ihre `<last 10 searches>` aufgeführt. Wenn Sie ein Element aus dieser Liste auswählen, wird automatisch erneut nach diesen Wörtern gesucht.

Sortieren

Klicken Sie auf **aufsteigend** oder **absteigend**, um die Tickets in der ausgewählten Spalte zu sortieren.

Felder...

Mit dieser Option kann jeder Benutzer die in der Tabelle angezeigten Spalten organisieren. Durch Klicken auf **Felder...** wird ein Dialogfeld in einem neuen Browser-Fenster geöffnet. Hier können Sie auswählen, welche Spalten ein- oder ausgeblendet werden und ihre Reihenfolge festlegen. Beliebige der folgenden Spalten können ein- oder ausgeblendet werden:

- **ID** – Eindeutige ID, die automatisch jedem Ticket zugewiesen wird.
- **Rechner-ID** – Das auf diesen Rechner angewendete Ticket.
- **Administrator** – Der Name des für die Lösung des Problems zuständigen Benutzers.
- **Kategorie** – Art des Problems, auf das in diesem Ticket eingegangen wird.
- **Status** – Offen, Warteliste, Geschlossen
- **Priorität** – Hoch, Normal, Niedrig
- **SLA-Typ** – Art des Service-Level-Agreements
- **Tech. senden** – Ja, Nein
- **Bestätigung** – Erforderlich, Nicht erforderlich
- **Arbeitsstunden** – Arbeitsstunden im Dezimalformat.
- **Letztes Änderungsdatum** – Zeitpunkt, zu dem zuletzt eine Anmerkung zu diesem Ticket hinzugefügt wurde.
- **Erstellungsdatum** – Zeitpunkt, zu dem das Ticket erstmals eingegeben wurde.
- **Fälligkeitsdatum** – Fälligkeitsdatum des Tickets.
- **Auflösungsdatum** – Datum, an dem das Ticket geschlossen wurde.
- **Absendername** – Person, die das Ticket eingesendet hat: Benutzer, Benutzername oder Rechner-ID.
- **Absender-E-Mail** – E-Mail-Adresse des Absenders.
- **Absender-Telefon** – Telefonnummer des Absenders.

Sie können auch weitere benutzerdefinierte Felder auswählen, die Sie zuvor mit "Ticketing > **Felder bearbeiten** *(siehe 471)*" erstellt haben.

Bei Feldänderungen automatisch einreichen/Einreichen

Wenn **Bei Feldänderungen automatisch einreichen** aktiviert ist, wird die Seite **Übersicht anzeigen** erneut angezeigt, wann immer ein Feld im **Listenfeld-Filter** geändert wird. Wenn diese Option nicht aktiviert ist, können Sie mehrere **Listenfeld-Filter** gleichzeitig ändern. Die Seite **Übersicht anzeigen** wird erst dann wieder angezeigt, wenn Sie auf **Einreichen** klicken.

(Listenfeld-Filter)

Jedes Feld des Typs `List`, wie beispielsweise **Kategorie**, **Status** oder **Priorität**, wird auch als

auswählbare Dropdown-Liste angezeigt. Wenn Sie Werte aus einer oder mehreren dieser Dropdown-Listen auswählen, wird der Seitenbereich gefiltert, sodass nur die Tickets angezeigt werden, die den ausgewählten Werten entsprechen. Benutzerdefinierte `List`-Felder werden unter "Ticketing > **Felder bearbeiten** *(siehe 471)*" erstellt.

Tickets ausblenden, die zuletzt geändert wurden nach dem/Einstellen

Stellen Sie das Datum und die Uhrzeit dieser Steuerung ein, um nur diejenigen Tickets anzuzeigen, die *vor* einem bestimmten Datum liegen.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Seite wählen

Wenn mehr Datenzeilen ausgewählt werden, als auf einer einzigen Seite angezeigt werden können, klicken Sie auf die Schaltflächen << und >>, um die vorherige und nächste Seite anzuzeigen. Die Dropdown-Liste führt alphabetisch den ersten Datensatz jeder Seite mit Daten auf.

Löschen...

Wählen Sie ein oder mehrere Tickets aus und klicken Sie auf **Löschen...**, um diese Tickets permanent aus dem System zu löschen. Gelöschte Tickets können nicht wiederhergestellt werden.

Archivieren...

Wählen Sie ein oder mehrere Tickets aus und klicken Sie auf **Archivieren...**. Archivierte Tickets verbleiben in der Datenbank, werden jedoch in separate Tabellen verschoben. Mit der Funktion Archivieren können Sie überflüssige oder alte Tickets aus der aktiven Datenbank herausnehmen, *ohne* sie vom System zu löschen. Sie können Tickets jederzeit zwischen der aktiven und der Archiv-Datenbanktabelle hin und her verschieben.

Archivierte Tickets anstelle aktiver Tickets anzeigen/Wiederherstellen

Aktivieren Sie das Kontrollkästchen **Archivierte Tickets anstelle aktiver Tickets anzeigen**, um nach archivierten Tickets zu suchen und sie zu prüfen. Mit der Schaltfläche **Wiederherstellen...** können Sie Tickets wieder in die aktive Tabelle verschieben.

Tickets migrieren

Ticketing > Tickets verwalten > Tickets migrieren

Auf der Seite **Tickets migrieren** können Sie zwei Aufgaben ausführen:

- Ausgewählte Tickets aus **Ticketing** zu **Service Desk**-Tickets migrieren
- **Service Desk**-Ticket-XMLs zu **Ticketing**-Tickets migrieren

Tickets aus Ticketing in Service Desk migrieren

Im Seitenbereich von **Tickets migrieren** werden alle Tickets angezeigt, die Sie auf der Seite "Ticketing > **Übersicht anzeigen** *(siehe 457)*" einsehen können.

1. Wählen Sie im Seitenbereich die Tickets aus, die Sie migrieren möchten. Klicken Sie auf **Alle auswählen**, um alle Tickets auszuwählen.
2. Klicken Sie auf **Migrieren**, um alle ausgewählten Tickets nach **Service Desk** zu migrieren.

Service Desk-Tickets in Ticketing importieren

1. Exportieren Sie ausgewählte Tickets nach **Service Desk** in eine XML-Datei auf Ihrem lokalen Rechner oder im Netzwerk über die Schaltfläche **Exportieren** unter "Service-Desk > **Tickets**".

2. Klicken Sie auf **Importieren** unter "Ticketing > **Tickets migrieren**" und wählen Sie die in Schritt 1 erstellte XML-Datei aus.

Benachrichtigungsrichtlinie

Ticketing > Ticketing konfigurieren > Benachrichtigungsrichtlinie

Auf der Seite **Benachrichtigungsrichtlinie** legen Sie fest, wann vom **Ticketing**-Modul E-Mail-Benachrichtigungen versendet werden. *Sie können für jede Rechnergruppe mehrere Regeln definieren, indem Sie auf die Schaltfläche* **Hinzufügen** *anstelle von* **Aktualisieren** *klicken.* Auf diese Weise können Sie für verschiedene Ticketing-Ereignisse unterschiedliche E-Mail-Listen erstellen. Sie können beispielsweise E-Mail-Benachrichtigungen an eine Gruppe von Benutzern bei der Erstellung von Tickets und beim Hinzufügen von Anmerkungen senden, jedoch bei überfälligen Tickets eine E-Mail an eine andere Liste von Benutzern versenden.

So stellen Sie ein, dass Ihnen eine E-Mail-Benachrichtigung für ein Ticketing-Ereignis gesendet wird:

1. Aktivieren Sie das Kontrollkästchen links von dem Ticketing-Ereignis, über das Sie benachrichtigt werden möchten.
2. Geben Sie eine kommagetrennte Liste der E-Mail-Adressen in das Bearbeitungsfeld **E-Mail-Liste** ein.
3. Aktivieren Sie das Kontrollkästchen links von den Gruppen-IDs, auf die diese Benachrichtigungsrichtlinie angewendet werden soll.
4. Klicken Sie auf die Schaltfläche **Aktualisieren** oder **Hinzufügen**.

Hinweis: Sie können *keine* Benachrichtigungen an die Ticket-Empfänger-E-Mail-Adresse senden, die unter "Ticketing > **E-Mail-Leseprogramm** *(siehe 472)*" festgelegt wurde.

Von-Adresse

Die von Ticketbenachrichtigungen verwendete `From`-Adresse ist die im **E-Mail-Leseprogramm** *(siehe 472)* festgelegte Adresse, sofern eine definiert wurde. Falls noch kein **E-Mail-Leseprogramm** definiert wurde, wird die `From`-Adresse aus "System > **Ausgehende E-Mail** *(siehe 446)*" verwendet.

Kontrollkästchen 'Benachrichtigungstyp'

In der nachstehenden Liste ist angegeben, wann das Ticketing-System eine E-Mail-Benachrichtigung *an alle E-Mail-Empfänger in der E-Mail-Liste* sendet.

- **Ticketerstellung** – Wenn diese Option aktiviert ist, wird zum Zeitpunkt der Ticketerstellung eine E-Mail gesendet.
- **Anmerkung ändern/hinzufügen** – Wenn aktiviert, wird eine E-Mail gesendet, wenn das Ticket geändert wird. Dazu gehört auch das Hinzufügen einer Anmerkung zu einem Ticket.
- **Überfälliges Ticket** – Wenn diese Option aktiviert ist, wird eine E-Mail gesendet, wenn eine Anmerkung bis zu ihrem Fälligkeitsdatum nicht geschlossen wurde.
- **Übersicht bearbeiten** – Wenn diese Option aktiviert ist, wird eine E-Mail gesendet, wann immer ein Benutzer die Übersichtszeile eines Tickets ändert. Klicken Sie auf **Format**, um das Format dieser E-Mail-Benachrichtigung zu bearbeiten.
- **Automatische Antwort an E-Mails senden, die neue Tickets erstellen** – Wenn diese Option aktiviert ist, wird eine automatische Antwortnachricht an die Person gesendet, die eine E-Mail gesendet hat, durch die ein neues Ticket generiert wurde. Mithilfe automatischer Antwortnachrichten erhalten Benutzer eine Bestätigung, dass ihre Anfrage erhalten und vom System verarbeitet wurde. Die Erstellung von Tickets basierend auf eingehenden E-Mails wird über **E-Mail-Leseprogramm** *(siehe 472)* und **E-Mail-Mapping** *(siehe 474)* konfiguriert. Klicken Sie auf **Format**, um das Format dieser E-Mail-Benachrichtigung zu bearbeiten.

- **Administrator-Änderung** – Wenn diese Option aktiviert ist, wird eine E-Mail gesendet, wenn ein Ticket einem anderen Benutzer zugewiesen wird. Klicken Sie auf **Format**, um das Format dieser E-Mail-Benachrichtigung zu bearbeiten.
- **Feldänderung** – Wenn diese Option aktiviert ist, wird eine E-Mail gesendet, wann immer ein Benutzer ein benutzerdefiniertes Feld in einem Ticket ändert. Klicken Sie auf **Format**, um das Format dieser E-Mail-Benachrichtigung zu bearbeiten.
- **Fälligkeitsdatumsänderung** – Wenn diese Option aktiviert ist, wird eine E-Mail gesendet, wann immer ein Benutzer das Fälligkeitsdatum eines Tickets ändert. Klicken Sie auf **Format**, um das Format dieser E-Mail-Benachrichtigung zu bearbeiten.
- **Ticketabsender benachrichtigen, wenn eine Anmerkung hinzugefügt wird** – Wenn diese Option aktiviert ist, wird zusätzlich zu der E-Mail-Liste für alle E-Mail-Benachrichtigungen auch eine E-Mail an die für den Ticketabsender eingegebene E-Mail-Adresse gesendet.
- **Alle öffentlichen Anmerkungen in Ändern/Benachrichtigung hinzufügen einschließen** – Wenn diese Option aktiviert ist, werden *alle* Anmerkungen für ein Ticket eingeschlossen, wenn eine **Anmerkung ändern/hinzufügen**-Nachricht abgesendet wird
- **Benachrichtigungen über erhaltene E-Mails immer an Bearbeiter senden** – Wenn diese Option aktiviert ist, erhält der Ticketbearbeiter eine E-Mail, wenn eine Antwort-E-Mail eingeht und dem Ticket hinzugefügt wird, selbst dann, wenn sich der Bearbeiter nicht in der E-Mail-Liste für Benachrichtigungen für diese Gruppen-ID befindet.
- **Automatische Antwort an E-Mails senden, die neue Tickets erstellen** – Wenn diese Option aktiviert ist, wird eine automatische Antwortnachricht an die Person gesendet, die eine E-Mail gesendet hat, durch die ein neues Ticket generiert wurde. Mithilfe automatischer Antwortnachrichten erhalten Benutzer eine Bestätigung, dass ihre Anfrage erhalten und vom System verarbeitet wurde. Die Erstellung von Tickets basierend auf eingehenden E-Mails wird über **E-Mail-Leseprogramm** *(siehe 472)* und **E-Mail-Mapping** *(siehe 474)* konfiguriert. Klicken Sie auf **Format**, um das Format dieser E-Mail-Benachrichtigung zu bearbeiten.

Hinweis: Die Schaltflächen **E-Mail formatieren** werden nur für Benutzer mit Masterrolle angezeigt.

Alle auswählen/Alle abwählen

Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.

Rechnergruppe

Listet Rechnergruppen auf. Alle Rechner-IDs sind mit einer Gruppen-ID und optional einer Untergruppen-ID verknüpft.

Ereignisse aktivieren TMOAFEDNIRS

Identifiziert die Ticketing-Ereignisse, die eine E-Mail-Benachrichtigung der in der Spalte **E-Mail-Liste** aufgeführten E-Mail-Empfänger auslösen.

E-Mail-Liste

Die Liste der E-Mail-Empfänger, die bei bestimmten Ticketing-Ereignissen für diese Gruppen-ID benachrichtigt werden.

Zugriffsrichtlinie

Ticketing > Ticketing konfigurieren > Zugriffsrichtlinie

Auf der Seite **Zugriffsregel** legen Sie fest, wer Felder in Tickets bearbeiten bzw. anzeigen kann. Für jede Benutzerrolle und für alle Rechnerbenutzer können unabhängige Regeln festgelegt werden. Rechnerbenutzer sehen nur Tickets, die ihrer Rechner-ID zugewiesen wurden. Benutzer ohne Master-Rolle sehen nur Tickets für Umfänge, zu deren Zugriff sie autorisiert sind.

Benutzer oder Rolle auswählen

Bevor Sie irgendwelche anderen Richtlinienoptionen festlegen, wählen Sie `<Users>` (d. h. alle Rechnerbenutzer) oder eine Benutzerrolle aus der Dropdown-Liste aus.

Zugriffsrechte

Die folgenden Zugriffsrechte gelten für *alle Rechnerbenutzer* oder für eine bestimmte *Benutzerrolle*, laut Angabe in **Benutzer oder Benutzergruppe auswählen**.

- **'Ticket löschen' aktivieren** – Wenn diese Option aktiviert ist, kann die ausgewählte Benutzerrolle über die Seite **Löschen/Archivieren** *(siehe 463)* gesamte Tickets löschen.
- **'Ticket bearbeiten' aktivieren, um Anmerkungen zu ändern/entfernen oder um die Übersichtszeile zu ändern (Das Hinzufügen neuer Anmerkungen ist immer aktiviert)** – Wenn diese Option aktiviert ist, kann die ausgewählte Benutzerrolle vorhandene Tickets bearbeiten oder die Übersichtszeile ändern.

  > **Hinweis:** Das Hinzufügen neuer Anmerkungen ist für alle Benutzergruppen immer aktiviert.

- **'Ticket verknüpfen mit'-Bearbeitung aktivieren** – Wenn diese Option aktiviert ist, kann die ausgewählte Benutzerrolle die Rechner-ID oder die mit einem Ticket verknüpfte Gruppe bearbeiten.
- **Bearbeiten der Absenderinformationen aktivieren** – Wenn diese Option aktiviert ist, können die Absenderinformationen bearbeitet werden.
- **'Fälligkeitsdatum bearbeiten' bei Bearbeitung von Trouble-Tickets aktivieren** – Wenn diese Option aktiviert ist, kann die ausgewählte Benutzerrolle das Fälligkeitsdatum des Tickets ändern.
- **'E-Mail-Benachrichtigungen abstellen' bei Bearbeitung von Trouble-Tickets aktivieren** – Wenn diese Option aktiviert ist, kann die ausgewählte Benutzerrolle E-Mail-Benachrichtigungen beim Ändern eines vorhandenen Tickets unterdrücken.
- **Ausgeblendete Anmerkungen anzeigen** – Wenn diese Option aktiviert ist, kann die ausgewählte Benutzerrolle ausgeblendete Anmerkungen anzeigen.

  > **Hinweis:** Ausgeblendete Anmerkungen können von Benutzern *niemals* angezeigt werden.

- **Ausgeblendete Anmerkungen-Status-Kontrollkästchen ändern** – Wenn diese Option für die ausgewählte Benutzerrolle aktiviert ist, wird für Anmerkungen auf der rechten Seite jeder Ticket-Anmerkung ein **Ausblenden**-Kontrollkästchen angezeigt. Durch Aktvieren/Deaktivieren des **Ausblenden**-Kontrollkästchens wird die Anmerkung aus- oder eingeblendet.
- **Automatisch neue Anmerkung bei jeder Feldänderung einfügen** – Wenn diese Option für die ausgewählte Benutzerrolle aktiviert ist, werden bei jeder Änderung eines Ticketfelds automatisch Anmerkungen eingefügt.
  - **Als ausgeblendete Anmerkung** – Wenn diese Option für die ausgewählte Benutzerrolle aktiviert ist, werden automatische Anmerkungen als ausgeblendete Anmerkungen hinzugefügt. Diese Regel gilt nur, wenn die Option **Automatisch neue Anmerkung bei jeder Feldänderung einfügen** aktiviert ist.
  - **Administrator gestatten, das Hinzufügen von automatischen Anmerkungen zu unterdrücken** – Hierdurch wird das Hinzufügen einer automatischen Anmerkung beim Ändern der Ticketeigenschaften unterdrückt, und es wird keine manuelle Anmerkung hinzugefügt.
- **Zugriff auf jedes Ticketfeld definieren** – Definiert den Zugriff auf jedes Feld für die ausgewählte Benutzerrolle. Felder werden mit **Felder bearbeiten** *(siehe 471)* erstellt. Es sind drei Ebenen des Zugriffs möglich:
  - **Voller Zugriff** – Der Benutzer kann dieses Feld in jedem Ticket anzeigen und ändern.
  - **Nur Ansicht** – Der Benutzer kann dieses Feld anzeigen, jedoch nicht seinen Wert ändern.
  - **Ausgeblendet** –Ausgeblendete Felder sind für den Benutzer nicht sichtbar.

Richtlinie über Bearbeiterzuordnung

Ticketing > Ticketing konfigurieren > Richtlinie über Bearbeiterzuordnung

Über die Seite **Richtlinie über Bearbeiterzuordnung** wird ein VSA-Benutzer automatisch einem neuen oder vorhandenen Ticket zugewiesen. Die Zuweisung erfolgt anhand der Kombination der Werte in den Feldern des Typs `List`, die für ein Ticket eingegeben wurden. Die `Listen`-Felder und ihre möglichen Werte werden über "Ticketing > **Felder bearbeiten** *(siehe 471)*" definiert. Diese Regel wird bei jedem Speichern des Tickets durchgesetzt.

Administratorregel überschreiben

Die **Administratorregel** kann auf der Seite **Erstellen/Anzeigen** *(siehe 460)* für ein bestimmtes Ticket überschrieben werden. Hierzu wechseln Sie das Symbol neben dem Feld **Administrator**, damit das Symbol angezeigt wird, und weisen dann manuell einen Benutzer zu.

Rangordnung

Die Rangordnung für die Regel*auswahl* basiert auf der alphabetischen Sortierfolge des Regel*namens*. Dieser bestimmt auch, wie die Regeln im Seitenbereich aufgelistet werden. Eine Regel namens `AAA` wird beispielsweise immer vor `BBB` ausgewählt, solange alle Felder in `AAA` den Einstellungen des Tickets entsprechen. Sie können die Regelauswahl *zwingen*, die von Ihnen bevorzugte Sortierfolge zu verwenden, indem Sie die Regeln entsprechend benennen. Sie können beispielsweise jedem Regelnamen ein numerisches Präfix wie z. B. 01, 02, 03 usw. voranstellen und dann die Sortierfolge entsprechend ändern. Um bestehende Regeln umzubenennen, wählen Sie das Bearbeitungssymbol neben einem Regelnamen aus, geben einen neuen Namen ein und klicken auf **Anwenden**.

Name der Richtlinie

Geben Sie den Namen der Administratorregel ein

Bearbeiter

Wählen Sie den Benutzer aus, dem Tickets zugewiesen werden, die der ausgewählten Kombination der Werte in den `Listen`-Feldern entsprechen.

Erstellen

Klicken Sie auf **Erstellen**, um die Administratorregel zu erstellen.

Listenfelder

Jedes Feld des Typs `List`, wie beispielsweise **Kategorie**, **Status** oder **Priorität**, wird auch als auswählbare Dropdown-Liste angezeigt. Wählen Sie Werte für ein oder mehrere Felder aus. Die Kombination der Werte in den Feldern des Typs `Liste`, die mit einem Bearbeiter verknüpft sind, bestimmt, welcher Bearbeiter einem neuen oder vorhandenen Ticket automatisch zugewiesen wird.

Fälligkeitsrichtlinie

Ticketing > Ticketing konfigurieren > Fälligkeitsrichtlinie

Über die Seite **Fälligkeitsregel** wird das Fälligkeitsdatum jedes **neuen Tickets** basierend auf den Feldwerten festgelegt. Für die Festlegung eines Fälligkeitsdatums kann eine beliebige Kombination von Feldern des Typs `List` definiert werden. Auf diese Weise können Sie das Fälligkeitsdatum eines neuen Tickets basierend auf der Dringlichkeit des Tickets und dem garantierten Diensteniveau festlegen. Definieren Sie beispielsweise ein neues `Listen`-Feld namens **Service-Level** mit den folgenden Werten: `Premium`, `Standard`, `Economy`. Erstellen Sie verschiedene Fälligkeitsregeln für jede Kombination. Zum Beispiel:

- Setzen Sie die Lösungszeit auf `1 Stunde`, wenn **Priorität** = `Hoch` und **Service-Level** = `Premium`.

- Setzen Sie die Lösungszeit auf `7 Tage`, wenn **Priorität** = `Normal` und **Service-Level** = `Economy`.

Beim Erstellen eines neuen Tickets wird das Fälligkeitsdatum durch Hinzufügen der Anzahl Stunden in der Regel zur aktuellen Zeit festgelegt.

> **Hinweis:** Das Fälligkeitsdatum eines **bestehenden Tickets** kann manuell mit **Erstellen/Anzeigen** *(siehe 460)* geändert werden.

Überfällige Tickets

Wenn ein Ticket überfällig ist, wird das Fälligkeitsdatum als fettgedruckter dunkelroter Text auf der Seite **Übersicht anzeigen** *(siehe 457)* und in **Ticketing** *(siehe 239)*-Berichten angezeigt. Es wird außerdem als roter Text in der Kopfzeile der Seite **Erstellen/Anzeigen** *(siehe 460)* angezeigt. Sie können unter "Ticketing > **Benachrichtigungsrichtlinie** *(siehe 466)*" wahlweise eine E-Mail für überfällige Tickets senden. Ein Ticket gilt als aufgelöst, wenn sein Status auf 'Geschlossen' eingestellt und das Auflösungsdatum aufgezeichnet wird.

Rangordnung

Die Rangordnung für die Regel*auswahl* basiert auf der alphabetischen Sortierfolge des Regel*namens*. Dieser bestimmt auch, wie die Regeln im Seitenbereich aufgelistet werden. Eine Regel namens `AAA` wird beispielsweise immer vor `BBB` ausgewählt, solange alle Felder in `AAA` den Einstellungen des Tickets entsprechen. Sie können die Regelauswahl *zwingen*, die von Ihnen bevorzugte Sortierfolge zu verwenden, indem Sie die Regeln entsprechend benennen. Sie können beispielsweise jedem Regelnamen ein numerisches Präfix wie z. B. 01, 02, 03 usw. voranstellen und dann die Sortierfolge entsprechend ändern. Um bestehende Regeln umzubenennen, wählen Sie das Bearbeitungssymbol neben einem Regelnamen aus, geben einen neuen Namen ein und klicken auf **Anwenden**.

Standarddauer zur Behebung von Tickets ohne Richtlinie

Geben Sie die Anzahl der Stunden oder Tage zum Auflösen von Tickets ein, wenn neue Tickets erstellt werden, die keiner Regel entsprechen.

Name der Richtlinie

Geben Sie einen Namen für eine neue oder ausgewählte Fälligkeitsregel ein.

Lösungszeit

Beim Erstellen neuer Tickets, die den Feldwerten in dieser Regel entsprechen, wird das Fälligkeitsdatum durch Hinzufügen der Anzahl Stunden oder Tage zur aktuellen Zeit festgelegt.

Felder

Wählen Sie Werte für ein oder mehrere Feld(er) des Typs `Liste` aus, denen ein neues Ticket entsprechen muss, damit das Fälligkeitsdatum für das neue Ticket automatisch festgelegt wird.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol, um eine Zeile im Seitenbereich zu löschen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um die Kopfzeilenparameter mit Werten aus dieser Zeile auszufüllen. Sie können diese Werte in der Kopfzeile bearbeiten und dann erneut anwenden. Die ausgewählte Zeile ist gelb markiert.

Name

Der Name der Fälligkeitsregel.

Zeit

Die zum aktuellen Datum und zur aktuellen Uhrzeit hinzugefügte Zeit, mit der die Fälligkeitsregel für

ein neues Ticket festgelegt wird.

Alle anderen Spalten

Die Werte der Listenfelder, für die eine Übereinstimmung erforderlich ist, um mit dieser Regel ein Fälligkeitsdatum für ein neues Ticket festzulegen. Die Pflege benutzerdefinierter `Listen`-Felder erfolgt über **Felder bearbeiten** *(siehe 471)*.

Felder bearbeiten

Ticketing > Ticketing konfigurieren > Felder bearbeiten

Auf der Seite **Felder bearbeiten** können Sie Felder erstellen, die zum Klassifizieren von Tickets und zum Festlegen der Standardwerte für diese Felder verwendet werden. Felder werden mit dem gesamten Ticket, und nicht mit den einzelnen Anmerkungen des Tickets verknüpft. Sie können die Feldbezeichnung ebenso wie die zutreffenden Werte jedes Felds, einschließlich der obligatorischen Felder *anpassen*. Die hier definierten Felder werden auf den folgenden Seiten angezeigt: **Übersicht anzeigen** *(siehe 457)*, **Ticket anzeigen** *(siehe 460)*, **Löschen/Archivieren** *(siehe 463)*, **Zugriffsregel** *(siehe 467)*, **Fälligkeitsregel** *(siehe 469)* und **E-Mail-Mapping** *(siehe 474)*.

Obligatorische Felder

Es gibt drei obligatorische Felder des Typs `Liste`, die nicht aus dem System entfernt werden dürfen. Die Werte dieser Felder können angepasst werden. Die obligatorischen Felder sind:

- **Kategorie** – Klassifiziert Tickets nach IT-Kategorie.
- **Status** – Status des aktuellen Tickets: `Offen`, `In Bearbeitung`, `Geschlossen`
- **Priorität** – `Hoch`, `Normal`, `Niedrig`

Nächste Ticket-ID einstellen auf N/Anwenden

Gibt die Ticketnummer des nächsten Tickets an. Zeigt die aktuelle "nächste" Ticketnummer an. Klicken Sie auf **Anwenden**, um die Änderungen zu bestätigen.

Feldposition

Klicken Sie auf die Pfeiltasten nach oben/unten links von der Feldbezeichnung, um die Anzeigeposition dieses Felds in **Tickets erstellen/anzeigen** *(siehe 460)* zu ändern.

Feldbezeichnung

Hier können Sie die Bezeichnung jedes beliebigen Felds ändern. Klicken Sie auf **Aktualisieren**, um die Änderung anzuwenden.

Typ

Geben Sie für jedes Feld den Datentyp an.

- `Zeichenfolge` – Kann Text bis zu einer Länge von 500 Zeichen enthalten. Eignet sich am besten für Angaben, wie die Position eines Problems oder andere Variablen, die nicht in die Übersichtszeile gehören.
- `Ganzzahl` – Kann positive oder negative ganzzahlige Werte enthalten.
- `Liste` – Hiermit können Sie eine Dropdown-Liste mit Optionen zur Auswahl erstellen. Die Optionen für Felder des Typs `Liste` werden durch Klicken auf den Wert `<Edit List>` in der Dropdown-Liste **Standardwert** bearbeitet.

> **Hinweis:** Nur Feldes des Typs `Liste` werden als auswählbare Dropdown-Liste angezeigt, in der Sie die Anzeige von Tickets auf den Seiten **Übersicht anzeigen** *(siehe 457)* und **Löschen/Archivieren** *(siehe 463)* filtern können.

- `Number (nn.d)` – Zahl mit immer einer Dezimalstelle
- `Number (nn.dd)` – Zahl mit immer zwei Dezimalstellen
- `Number (nn.ddd)` – Zahl mit immer drei Dezimalstellen
- `Number (nn.dddd)` – Zahl mit immer vier Dezimalstellen

Standardwert

Beim Erstellen eines Tickets wird automatisch jedes Feld auf seinen Standardwert eingestellt. Diesen Standardwert können Sie hier angeben.

> **Hinweis:** Standardwerte gelten systemweit und sind für alle Rechnergruppen-IDs und Benutzerrollen immer gleich.
>
> **Hinweis:** Mit **E-Mail-Mapping** *(siehe 474)* können die hier ausgewählten Standardwerte für unter **E-Mail-Leseprogramm** *(siehe 472)* erstellte Tickets geändert werden.

<Liste bearbeiten>

Dieser Wert wird in der Dropdown-Liste für ein Feld des Typs `List` in der Spalte **Standardwert** angezeigt. Klicken Sie auf `<Edit List>`, um die Liste der Werte für dieses Feld zu bearbeiten.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um die Änderungen an Feldbezeichnungen, Standardwerten oder `List`-Werten zu bestätigen.

Neu

Klicken Sie auf **Neu**, um ein neues Feld zu erstellen.

E-Mail-Leseprogramm

Ticketing > Ticketing konfigurieren > E-Mail-Leseprogramm

Auf der Seite **E-Mail-Leseprogramm** legen Sie ein POP3-E-Mail-Konto für periodisches Polling fest. Die vom POP3-Server abgerufenen E-Mail-Nachrichten werden gemäß **E-Mail-Mapping** *(siehe 474)* klassifiziert und in Tickets konvertiert.

Integration von Alarmen und Tickets

Wenn ein VSA-Benutzer irgendwo im System auf den Link `New Ticket...` (üblicherweise für Alarme) klickt, wird die Aktion vom **Ticketing**-Modul in ein Ticket konvertiert. Dazu muss das E-Mail-Leseprogramm für **Ticketing** nicht aktiviert sein.

> **Hinweis:** Wenn das **Service Desk**-Modul installiert ist, finden Sie weitere Informationen unter "Service-Desk > **Service-Desk-Integration aktivieren** *(http://help.kaseya.com/webhelp/DE/KSD/7000000/index.asp#5478.htm)*".

Inhalt der E-Mail

Das **E-Mail-Leseprogramm** kann beliebige E-Mail-Nachrichten mit oder ohne Anhänge empfangen und ihre Inhalte im Ticketing-System hinzufügen. Es können weitere Informationen zu der E-Mail hinzugefügt werden, um die Zuordnung der E-Mail zum Ticketing-System zu verbessern. Die folgenden Tags können in den *Betreff oder Textkörper* der E-Mail eingeschlossen werden.

- `~ticrefid='xxx'` – Hängt den Textkörper der E-Mail-Nachricht an ein vorhandenes Ticket an, statt ein neues Ticket zu erstellen.
- `~username=’xxx’` – Fügt den mit `xxx` angegebenen Wert automatisch in das Feld **Absendername** ein.

> **Hinweis:** Wenn `~username='xxx'` *nicht* im Betreff oder Textkörper der E-Mail vorhanden ist, wird die `From`-Adresse des E-Mail-Absenders in das Feld **Absendername** eingetragen.

- `~useremail='xxx'` – Fügt den mit `xxx` angegebenen Wert automatisch in das Feld **Absender-E-Mail** ein.
- `~userphone='xxx` – Fügt den mit `xxx` angegebenen Wert automatisch in das Feld **Absender-Telefon** ein.
- `~category='xxx'` – Weist das erstellte Ticket einer bestimmten Kategorie zu. Die Kategorie muss bereits vorhanden sein.
- `~priority='xxx'` – Weist das erstellte Ticket einer bestimmten Priorität zu. Die Priorität muss bereits vorhanden sein.
- `~status='xxx'` – Weist das erstellte Ticket einem bestimmten Status zu. Der Status muss bereits vorhanden sein.
- `~assignee='xxx'` – Weist das erstellte Ticket einem bestimmten Benutzer zu. Der Benutzer muss bereits vorhanden sein.
- `~machineid='xxx.xxx'` – Weist das erstellte Ticket einer Rechner-ID zu. Die Rechner-ID muss bereits vorhanden sein. Wenn diese Informationen nicht vorhanden sind und die Tickets nicht mit **E-Mail-Mapping** *(siehe 474)* einer Rechner-ID oder Gruppen-ID zugewiesen werden, werden die Tickets standardmäßig der Gruppe `unnamed` zugewiesen.
- `~fieldName='xxx'` – Weist den Wert `xxx` einem beliebigen definierten Feld zu. Wenn dieses Feld vom Typ `List` ist, muss der Wert in der Liste vorhanden sein.

Unterdrückte Anmerkungen

Anmerkungen werden unterdrückt, wenn eine E-Mail ohne Textkörper und ohne Anhänge gesendet wird oder wenn in eine Antwort-E-Mail kein Antworttext eingeschlossen ist.

E-Mail-Leseprogramm-Meldungen

Sie können per E-Mail benachrichtigt werden, wenn "Ticketing > E-Mail-Leseprogramm" fehlschlägt. Dies legen Sie unter "Monitor > **Meldungen – System** *(siehe 314)*" fest.

E-Mail-Adresse

Geben Sie die E-Mail-Adresse ein, von der Sie periodisch E-Mail-Nachrichten abrufen möchten. Antworten an diese E-Mail-Adresse werden vom Ticketing-System verarbeitet und als Anmerkungen zum jeweiligen Ticket hinzugefügt.

E-Mail-Leseprogramm deaktivieren

Aktivieren Sie dieses Kontrollkästchen, wenn das E-Mail-Leseprogramm nicht in der Lage sein soll, einen Server zu pollen.

Protokoll anzeigen

Klicken Sie auf **Protokoll anzeigen**, um das Polling-Protokoll für dieses E-Mail-Leseprogramm zu überprüfen.

Unabhängige Ticket-Sequenz-Nummerierung abbrechen (Identitätswert verwenden)

Gilt nur für "Vor-Ort"-Umgebungen mit einer einzelnen **Partition** *(siehe 631)*; wenn aktiviert, stimmen die Ticketnummern mit jenen in ausgehenden E-Mails überein. Wenn nicht aktiviert, können die beiden Nummern voneinander abweichen. In zusätzlichen Partitionen stimmen die Nummern immer überein.

Hostname

Der Name des POP3-Hostdienstes muss angegeben werden. POP3 ist das einzige unterstützte E-Mail-Protokoll. Ein Beispiel wäre `pop.gmail.com`.

Port

Geben Sie die vom POP3-Dienst verwendete Portnummer an. Normalerweise haben die Nicht-SSL POP3-Ports die Nummer 110 und die SSL POP3-Ports die Nummer 995.

SSL verwenden

Aktivieren Sie dieses Kontrollkästchen, um SSL-Verbindungen mit Ihrem POP-Server zu ermöglichen Damit diese Funktion verwendet werden kann, muss Ihr POP-Server SSL unterstützen. Normalerweise verwenden POP3-Server mit aktiviertem SSL den Port 995.

Login

Geben Sie den Namen des E-Mail-Kontos ein. Der @ Domain-Name sollte nicht in den Kontonamen eingeschlossen werden. Falls die **E-Mail-Adresse** beispielsweise `jsmith@acme.com` lautet, geben Sie `jsmith` als Kontonamen ein.

Passwort

Geben Sie das Passwort des E-Mail-Kontos ein.

Auf neue E-Mails prüfen alle <N> Minuten

Die Anzahl Minuten, die das **E-Mail-Leseprogramm** warten sollte, bevor es den POP3-Server auf neue E-Mails pollt.

Lehnen Sie eingehende E-Mails mit folgender Betreffzeile ab

Diese Option wird nur für **Masterrollenbenutzer** *(siehe 616)* angezeigt. Geben Sie Text ein, um eingehende E-Mails, die diesen Text *in der Betreffzeile* enthalten, zu ignorieren. Hierbei wird nicht zwischen Groß- und Kleinschreibung unterschieden. *Anführungs- und Platzhalterzeichen, wie * und ? werden im wörtlichen Sinn als Teil des Zeichenfolgeninhalts interpretiert.* Erstellen Sie mehrere Filter durch Verwendung mehrerer Zeilen. Mehrere Filter werden als ODER-Anweisungen interpretiert. Vor und nach ganzen Wörtern sollte jeweils ein Leerzeichen eingegeben werden. Beispiel:

```
Undeliverable
Do not reply
```

Diese Liste der zu ignorierenden Ausdrücke kann auch auf der Seite "Ticketing > **E-Mail-Leseprogramm** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#434.htm)*" und auf der Registerkarte "Service-Desk > Einstellungen für eingehende E-Mails und Alarme > Allgemein" gepflegt werden. Manuell können Sie die Liste über die Datei `<Kaseya_Installation_Directory>\Kaseya\KServer\ignoreSubject.txt` bearbeiten.

Anwenden

Klicken Sie auf **Anwenden**, um das E-Mail-Leseprogramm zu verwenden

Jetzt verbinden

Klicken Sie auf **Jetzt verbinden**, um sofort eine Verbindung zum POP3-Server herzustellen, anstatt bis zur nächsten Pollingzeit zu warten. Hiermit können Sie die Konfiguration des E-Mail-Leseprogramms testen.

E-Mail-Mapping

Ticketing > Ticketing konfigurieren > E-Mail-Mapping

Auf der Seite **E-Mail-Mapping** weisen Sie Standardwerte für **neue Tickets** zu, die mit dem **E-Mail-Leseprogramm** *(siehe 472)* erstellt wurden. Die zugewiesenen Standardwerte basieren auf der E-Mail-Adresse oder der E-Mail-Domain des *Absenders* der E-Mail. Die Abstimmung kann wahlweise nach dem in die Betreffzeile der E-Mail eingegebenen Text gefiltert werden. Diese Informationen

überschreiben die mit **Felder bearbeiten** *(siehe 471)* definierten Standardwerte.

E-Mail-Adresse oder Domäne

Die E-Mail-Adresse oder Domain *des Absenders*. Zum Beispiel: `jsmith@acme.com` oder `acme.com`.

Schema für nicht zugewiesene E-Mails einstellen

Wenn diese Option aktiviert ist, werden Standard-Feldwerte für eingehende E-Mails zugewiesen, die von keinem anderen E-Mail-Abbild abgedeckt werden

Betreffzeilenfilter

Weist Ticket-Standardwerte zu, wenn die *E-Mail-Betreffzeile der Filterzeichenfolge entspricht*. Hierbei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Platzhalterzeichen werden nicht unterstützt. Ein einzelnes * ohne andere Zeichen in dem Filter bedeutet, dass alles durchgelassen wird. Boolesche Anweisungen werden nicht akzeptiert.

Abbild verknüpfen mit

Klicken Sie auf den Link **Verknüpfung auswählen**, um neue Tickets, die mit diesem Abbild erstellt wurden, mit einer Rechner-ID, Rechnergruppe, Organisation, Abteilung oder einem Mitarbeiter zu verknüpfen.

Bearbeiter

Geben Sie den Namen des VSA-Benutzers ein, der neuen Tickets zugewiesen wird, die mit dieser E-Mail-Zuordnung erstellt wurden.

Felder

Geben Sie die Standard-Feldwerte an, die neuen Tickets zugewiesen werden, die erstellt werden, wenn eine E-Mail vom Ticketing-System über dieses Abbild erhalten wird.

Erstellen

Klicken Sie auf **Erstellen**, um ein neues E-Mail-Abbild unter Verwendung der zuvor ausgewählten Kopfzeilenwerte zu erstellen.

Löschen-Symbol

Klicken Sie auf das Löschen-Symbol, um diesen Datensatz zu löschen.

Bearbeitungssymbol

Klicken Sie auf das Bearbeitungssymbol einer Zeile, um automatisch Kopfzeilenparameter festzulegen, die mit jenen der ausgewählten Rechner-ID übereinstimmen.

Kapitel 11

Datenbanksichten

In diesem Kapitel

Datenbankansichten und -funktionen

System > Datenbankzugriff > Datenbankansichten

Das System zeigt eine Reihe von **Datenbankansichten und Datenbankfunktionen** *(siehe 484)* an, über die Clients auf Daten im Kaseya-Repository direkt zugreifen können. Die Datenbankansichten können als parametrisierte Ansichten aufgefasst werden. Sie können diese Ansichten dazu verwenden, Daten in ein Arbeitsblatt zur Analyse zu übertragen und Berichte vorzubereiten In diesem Dokument werden die Ansichten und Funktionen näher beschrieben, und es werden zwei Beispielanwendungen vorgestellt, **Crystal Reporting** *(siehe 480)* und **Microsoft Excel** *(siehe 479)*. Kaseya gibt kein Expertenwissen in der Verwendung von Excel oder Crystal vor. Diese Beispiele sollen Ihnen die Grundlagen vermitteln und Ihnen beim Einstieg helfen. Für Produktschulung durch Drittanbieter oder bei weiteren Fragen wenden Sie sich an den Hersteller des Drittanbietertools. In einem Anhang zu diesen Dokumenten finden Sie für jedes einzelne Feld eine Beschreibung der Inhalte der Ansichten und Funktionen.

Die bereitgestellten Ansichten können in **vier Gruppen von Datenbankansichten** *(siehe 484)* unterteilt werden.

- Die erste Gruppe bietet Informationen zu allen überwachten **Rechnern**.
- Die zweite Gruppe bietet Informationen zu **Aktivitäten und zum aktuellen Status** wesentlicher Teile des Systems.
- Die dritte Gruppe enthält Informationen zum **Ticketing**-System.
- Die vierte Gruppe enthält Informationen zu den **Monitoring**-Alarmen.

Zugriff auf Datenbankansichten

Die Datenbankansichten werden jedes Mal installiert, wenn die Aktion **Schema erneut anwenden** ergriffen wird. Zum Zugriff auf diese Ansichten wird eine einzelne Datenbankbenutzer-ID, `KaseyaViews`, bereitgestellt.

1. Aus Sicherheitsgründen müssen Sie zuerst das Kennwort für die `KaseyaViews`-Benutzer-ID erstellen oder ändern, indem Sie das Kennwort auf der Seite System > **Datenbankansichten** eingeben.
2. Ab diesem Punkt können Sie externe Anwendungen wie Crystal Reports oder Excel verwenden, um die Datenbankansichten über die eingegebene `KaseyaViews`-Benutzer-ID und das Kennwort direkt aufzurufen.

Nutzung in Excel

Datenquelle in Windows erstellen

Microsoft Excel kann auf die Ansichten durch Einrichten einer Datenquelle zugreifen. Eine Datenquelle ist eine Kerndefinition innerhalb von Microsoft. Die meisten Microsoft-Produkte verfügen über Funktionen, um über eine Datenquelldefinition auf Daten zuzugreifen. Sie erstellen eine Datenquelle durch Auswahl von 'Einstellungen' auf der Startschaltfläche. Wählen Sie unter 'Einstellungen' die Systemsteuerung. In der Systemsteuerung wählen Sie 'Verwaltung'. Über dieses Menü kann eine Datenquelle erstellt werden.

Die Datenquelle sollte als ein System DSN eingerichtet werden. Über dieses Dialogfeld erstellen Sie eine Quelle unter Verwendung des SQL-Server-Treibers. Für die Einrichtung wird der Name des Datenbankservers (für gewöhnlich der ComputerName), die Benutzer-ID (KaseyaViews) und das Kennwort sowie der Name des Datenbankschemas (ksubscribers) benötigt.

Datenquelle in Excel auswählen

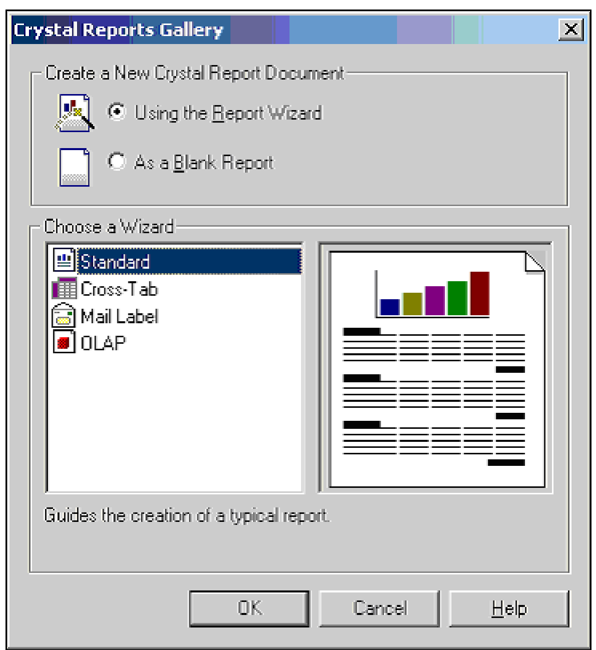
Sobald eine Datenquelle erstellt wurde, kann von Excel aus darauf verwiesen werden. Öffnen Sie ein leeres Arbeitsblatt und wählen Sie die Option **Daten > Externe Daten > Neue Abfrage erstellen...** Der

Benutzer wird zur Eingabe der Anmeldedaten für die Datenbank aufgefordert. Sobald diese Anforderung erfüllt ist, kann eine Ansicht ausgewählt werden. Nun kann eine SQL-Abfrage erstellt werden, um Informationen direkt in Excel zu übertragen.

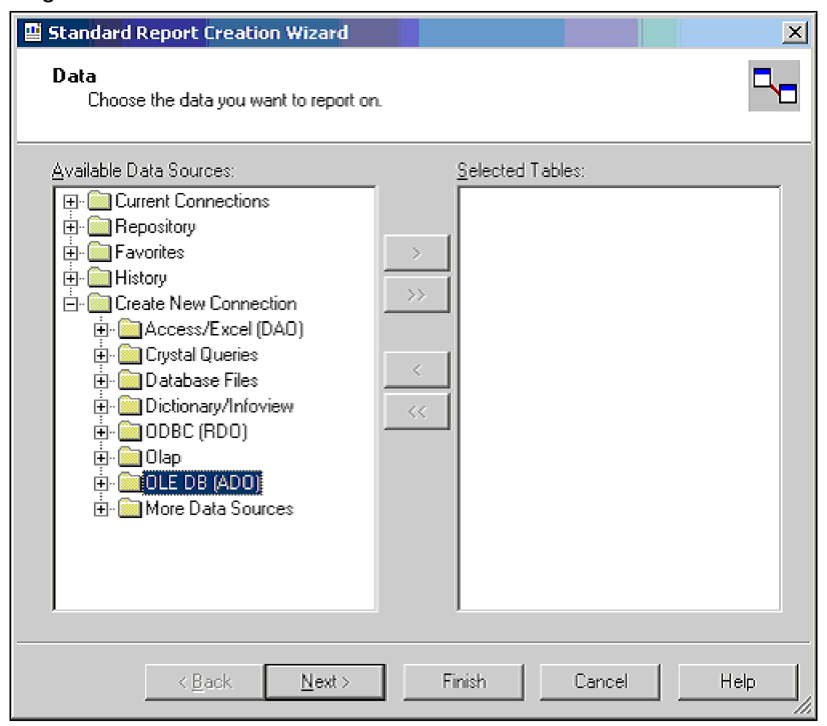
Nutzung der Crystal-Berichte

Über Crystal-Berichte können clientspezifische Berichte erstellt werden. Mit Crystal 9 und 10 können verschiedene Ausgabeformate, einschließlich PDF, Word und Excel, produziert werden. Zum Einrichten eines Berichts kann der Crystal-Berichtsassistent verwendet werden. Dieser Prozess beginnt mit dem folgenden Dialogfeld.

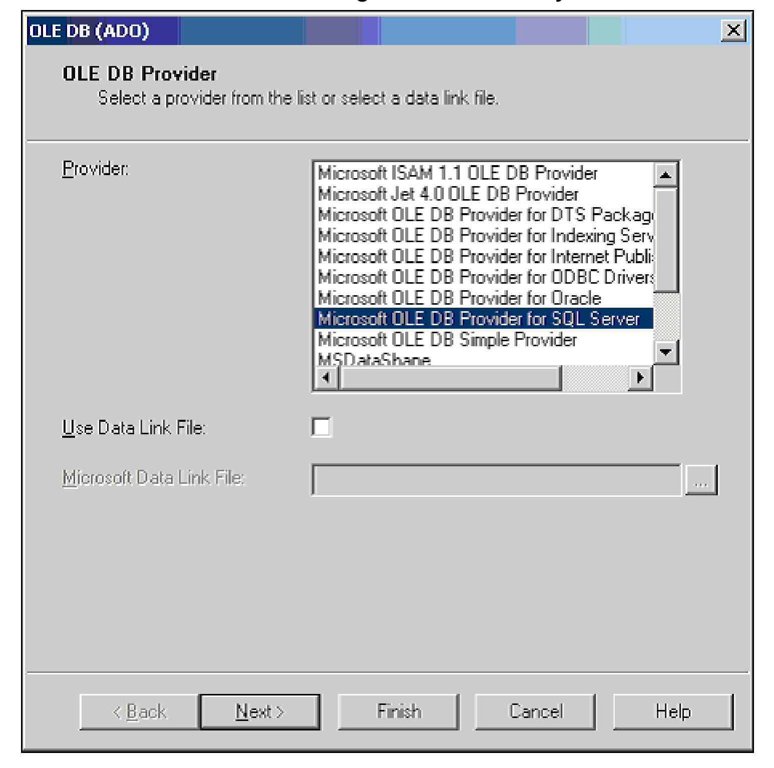
1. Der Client wählt ein Berichtsformat. Für dieses Beispiel wird das Standardformat verwendet.



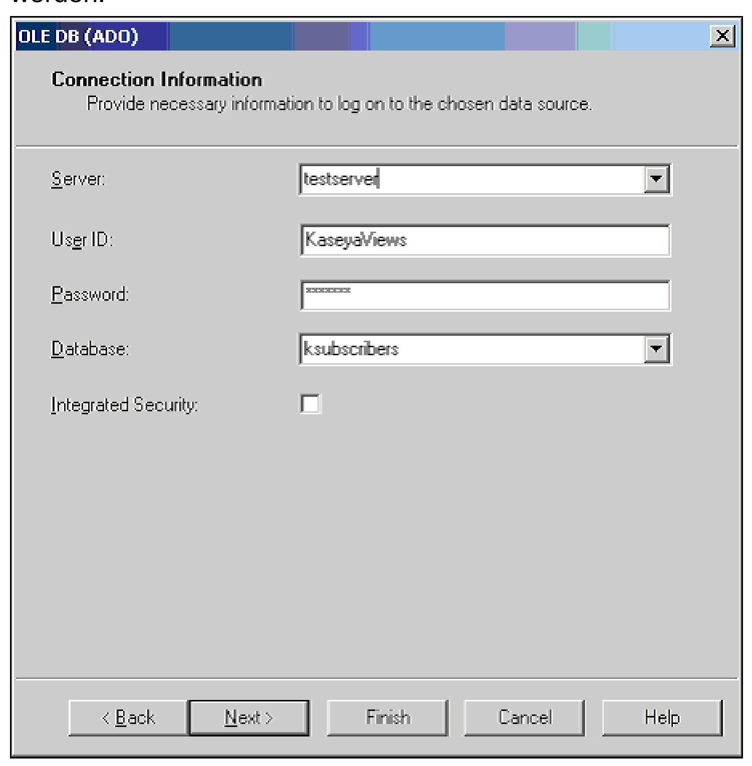
2. Als nächstes wird die Datenquelle ausgewählt. Hierzu bestimmen Sie zunächst eine Zugriffsmethode. Wählen Sie ADO aus.



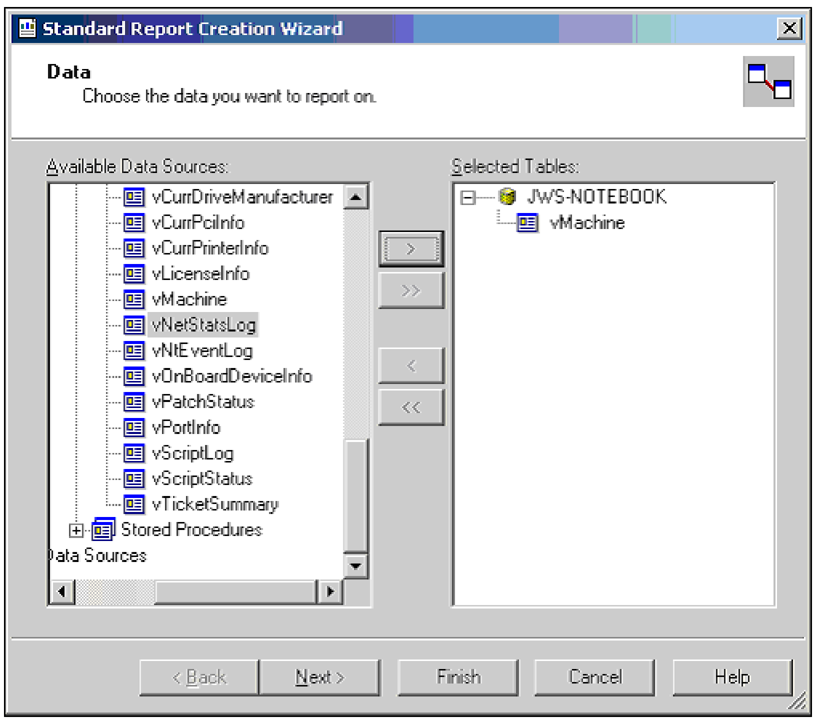
3. Nachdem ADO festgelegt wurde, kann der SQL-Server-Treiber ausgewählt werden. Dies ist die korrekte Auswahl für den Zugriff auf die Kaseya-Datenbank.



4. Im nächsten Schritt stellen Sie die Anmeldedaten für die Verbindung zur Datenbank bereit. Wie in diesem Dialogfeld gezeigt, müssen Server, Benutzer-ID, Kennwort und Datenbank angegeben werden.

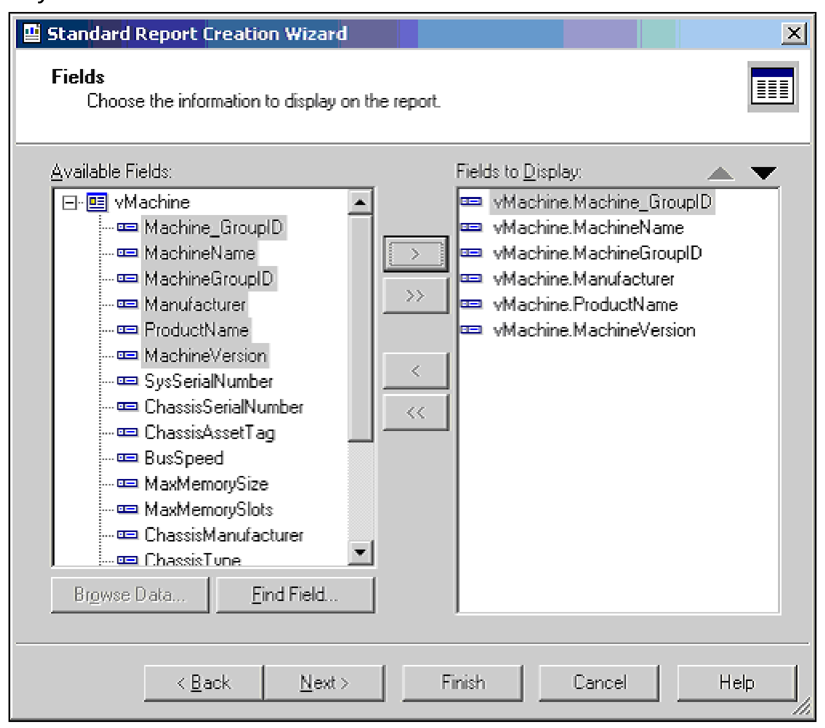


5. Sobald die Anmeldedaten bereitgestellt wurden, werden alle verfügbaren Ansichten angezeigt. Wählen Sie daraus eine oder mehrere für den gewünschten Bericht aus.

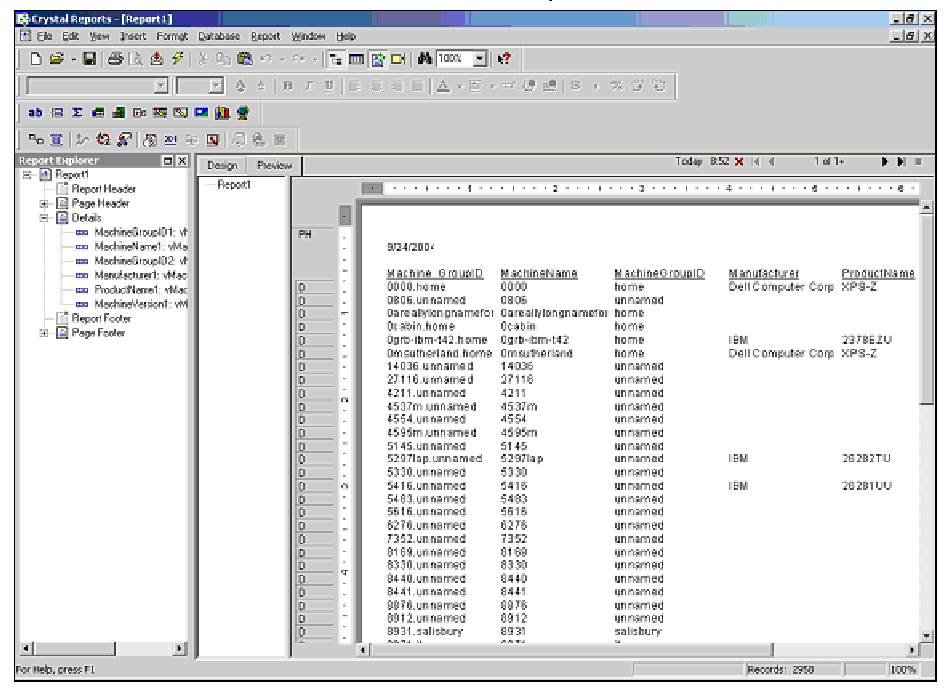


6. Nachdem eine Ansicht ausgewählt wurde, können die einzuschließenden Spalten ausgewählt werden. Crystal bietet mehrere Möglichkeiten, diese Daten zu formatieren. Auf diese Optionen

wird in diesem Dokument nicht näher eingegangen. Für diese Informationen sollte die Crystal-Dokumentation konsultiert werden.



7. Der resultierende Bericht kann gedruckt oder per E-Mail an die zutreffende Zielgruppe gesendet werden. Das Format des Berichts kann frei gewählt werden. Über diese Funktion kann eine PDF-Datei oder eine Reihe anderer Formate produziert werden.



Bereitgestellte Ansichten und Funktionen

Hinweis: Ansichten können mit den API-Webdienstvorgängen **GetPublishedViews** *(siehe 566)*, **GetPublishedViewRows** *(siehe 564)*, and **GetPublishedViewColumns** *(siehe 563)* zurückgegeben werden.

Hinweis: Mit einem Flaggensymbol markierte Elemente sind parametrisierte Funktionen, die nicht über die oben beschriebenen API-Webdienstvorgänge verfügbar sind. Lokale Benutzer können auf diese mit dem Flaggensymbol markierten Funktionen über SQL Server zugreifen.

Rechnergruppe	
vAddRemoveList *(siehe 487)*	Von der letzten Inventarisierung zurückgegebene Anwendungsliste hinzufügen/entfernen.
vBaseApplicationInfo *(siehe 492)*	Die Basisliste von Anwendungen auf einem Client-Desktoprechner.
vBaseCpuInfo *(siehe 493)*	Die Basisliste von CPUs auf einem Client-Desktoprechner.
vBaseDiskInfo *(siehe 493)*	Die Basisliste von Festplatten auf einem Client-Desktoprechner.
vBaseDriveManufacturer *(siehe 494)*	Die Basisliste der Hersteller der Festplatten auf einem Client-Desktoprechner.
vBasePciInfo *(siehe 494)*	Die Basisliste von PCI-Karten auf einem Client-Desktoprechner.
vBasePrinterInfo *(siehe 495)*	Die Basisliste von Druckern auf einem Client-Desktoprechner.
vCollectionMember *(siehe 495)*	Liste der Obergruppen, der die einzelnen Rechner-IDs angehören (falls zutreffend)
vCurrApplicationInfo *(siehe 492)*	Die aktuelle Liste von Anwendungen auf einem Client-Desktoprechner.
vCurrCpuInfo *(siehe 493)*	Die aktuelle Liste von CPUs auf einem Client-Desktoprechner.
vCurrDiskInfo *(siehe 493)*	Die aktuelle Liste von Festplatten auf einem Client-Desktoprechner.
vCurrDriveManufacturer *(siehe 494)*	Die aktuelle Liste der Hersteller der Festplatten auf einem Client-Desktoprechner.
vCurrPciInfo *(siehe 494)*	Die aktuelle Liste von PCI-Karten auf einem Client-Desktoprechner.
vCurrPrinterInfo *(siehe 495)*	Die aktuelle Liste von Druckern auf einem Client-Desktoprechner.
vLicenseInfo *(siehe 501)*	Die Lizenzen der Anwendungen auf diesem Rechner.
vMachine *(siehe 501)*	Die über jeden Client-Desktoprechner bekannten Informationen
vOnBoardDeviceInfo *(siehe 510)*	Die aktuelle Liste von Platinengeräten auf einem Client-Desktoprechner.
vPortInf *(siehe 522)*	Die aktuelle Liste von Anschlüssen auf einem Client-Desktoprechner.
vSystemInfo *(siehe 524)*	Über die Funktion Audit > **Systeminformationen** *(siehe 154)* gesammelte Daten
vSystemInfoManual *(siehe 525)*	Der Funktion Systeminformationen zugefügte benutzerdefinierte Felder und Werte
vUptimeHistory *(siehe 527)*	Die für den Laufzeit-Historie-Bericht erfassten Daten. Wird in Verbindung mit dem getMachUptime-Webdienst verwendet.
vvProAssetDetails *(siehe 528)*	Listet Informationen über einen vPro-aktivierten Rechner auf, einschließlich der Herstellerangaben zur Hauptplatine.
Aktivität/Statusgruppe	
fnMissingPatchCounts_UsePolicy *(siehe 486)*	Gibt die Anzahl der Patches unter Verwendung der Patch-Bestätigungsrichtlinien für die angegebene Rechnergruppe zurück. Tabellendaten gemäß Anzeige in den Kreisdiagrammen für fehlende Patches in den Executive-Übersichtsberichten und auf der Seite 'Dashboard anzeigen' auf der Start-Registerkarte. Es wird nur jeweils eine Zeile zurückgegeben.

fnMissingPatchCounts_NoPolicy *(siehe 486)*	Gibt die Anzahl der Patches ohne Verwendung der Patch-Bestätigungsrichtlinien für die angegebene Rechnergruppe zurück. Tabellendaten gemäß Anzeige in den Kreisdiagrammen für fehlende Patches auf der Seite 'Dashboard anzeigen' auf der Start-Registerkarte. Es wird nur jeweils eine Zeile zurückgegeben.
fnOSCounts *(siehe 487)*	Gibt die Berichtssystemtypen und deren Anzahl für die angegebene Rechnergruppe zurück. Tabellendaten gemäß Anzeige in den Betriebssystem-Kreisdiagrammen in den Executive-Übersichtsberichten und auf der Seite 'Dashboard anzeigen' auf der Start-Registerkarte. Gibt eine Zeile für jeden Betriebssystemtyp zurück.
vAdminNotesLog *(siehe 488)*	Anmerkungen, die jeder Administrator manuell für einen Rechner oder eine Gruppe von Rechnern eingibt. Die Einträge in diesem Protokoll verfallen nie.
vAgentConfiguration *(siehe 488)*	Listet Agent-spezifische Konfigurationsdaten auf.
vAgentLabel *(siehe 489)*	Gibt den Status der Agents an. Wird für Anzeigezwecke verwendet.
vAlertLog *(siehe 490)*	Protokoll aller Meldungen, die per E-Mail versendet wurden. Mehrere Zeilen pro Rechner.
vBackupLog *(siehe 491)*	Protokoll aller Sicherungsereignisse.
vConfigLog *(siehe 496)*	Protokoll aller Konfigurationsänderungen. Nur ein Eintrag pro Änderung.
vEventDetail *(siehe 496)*	Liefert eine Beschreibung eines Ereignisses.
vEventInstanceDetail *(siehe 498)*	Liefert eine Beschreibung einer ausgelösten Ereignisinstanz.
vEventInstanceHistoryDetail *(siehe 499)*	Liefert einen Verlauf von ausgelösten Ereignisinstanzen.
vNetStatsLog *(siehe 509)*	Protokoll der Netzwerkstatistiken vom Agent.
vNtEventLog *(siehe 510)*	NT Event-Protokolldaten, die von jedem verwalteten Rechner erfasst wurden.
vPatchApprovalPolicyStatus *(siehe 511)*	Der Patch-Bestätigungsstatus eines Patch nach Patch-Richtlinie.
vPatchApprovalStatus *(siehe 512)*	Zeigt den Bestätigungsstatus eines Patch. Eine Zeile pro aktivem Patch.
vPatchPieChartCountsNoPolicy *(siehe 515)*	Gibt die Anzahl der Patches für Rechner ohne eine zugewiesene Richtlinie an.
vPatchPieChartCountsUsePolicy *(siehe 515)*	Gibt die Anzahl der Patches für Rechner mit einer zugewiesenen Richtlinie an.
vPatchPolicy *(siehe 516)*	Zeigt den Bestätigungsstatus eines Patch. Eine Zeile pro aktivem Patch in jeder Patch-Richtlinie.
vPatchPolicyMember *(siehe 517)*	Listet alle Patch-Richtlinien auf, denen die einzelnen Rechner-IDs angehören, falls zutreffend.
vPatchStatus *(siehe 518)*	Informationen zum Status aller Patches auf Rechnerbasis. Eine Zeile pro Rechner.
vPatchStatusByAgent *(siehe 520)*	Beschreibt den Patch-Status eines einzelnen Agent-Rechners.
vScriptLog *(siehe 523)*	Protokoll der Verfahrensausführungen aus Sicht des Kaseya Server.
vScriptStatus *(siehe 523)*	Verfahrensstatus für jeden Client.
Ticketing-Gruppe	
vTicketSummary *(siehe 527)*	Übersicht über Trouble-Tickets. Eine Zeile pro Ticket. Für die Namen, die in der Ansichts-Übersichtstabelle angezeigt werden, werden Spaltennamen verwendet.
vTicketNote *(siehe 526)*	Die mit einem Ticket verknüpften Anmerkungen. Möglicherweise mehrere Zeilen pro Ticket.

vTicketField *(siehe 526)*	Die mit einem Ticket verknüpften Felder. Die Standardfehler Kategorie, Status und Priorität sind immer an ein Ticket angehängt. Hinzugefügte Benutzerfelder werden ebenfalls in diese Ansicht eingeschlossen.
Monitoralarm-Gruppe	
vMonitorAlarmAlert *(siehe 504)*	Die aktuelle Liste der Alarme für alle Meldungen.
vMonitorAlarmCounter *(siehe 505)*	Die aktuelle Liste der Alarme für alle Monitorzähler.
vMonitorAlarmProcess *(siehe 506)*	Die aktuelle Liste der Alarme für alle Monitorprozesse.
vMonitorAlarmService *(siehe 506)*	Die aktuelle Liste der Alarme für alle Monitordienste.
vMonitorAlarmSNMP *(siehe 507)*	Die aktuelle Liste der Alarme für alle Monitor-SNMP-Abrufobjekte.
vMonitorAlarmSystemCheck *(siehe 508)*	Die aktuelle Liste der Alarme für alle Systemprüfungen.

fnMissingPatchCounts_UsePolicy / fnMissingPatchCounts_NoPolicy

Diese beiden Funktionen verwenden die gleichen Parameter und geben die gleichen Spalten zurück. Doch jede verwendet eine andere Filterung basierend auf den Patch-Bestätigungsrichtlinien.

fnMissingPatchCounts_UsePolicy	Gibt die Anzahl der Patches unter Verwendung der Patch-Bestätigungsrichtlinien für die angegebene Rechnergruppe zurück. Tabellendaten gemäß Anzeige in den Kreisdiagrammen für fehlende Patches in den Executive-Übersichtsberichten und auf der Seite 'Dashboard anzeigen' auf der Start-Registerkarte. Es wird nur jeweils eine Zeile zurückgegeben.	
fnMissingPatchCounts_NoPolicy	Gibt die Anzahl der Patches ohne Verwendung der Patch-Bestätigungsrichtlinien für die angegebene Rechnergruppe zurück. Tabellendaten gemäß Anzeige in den Kreisdiagrammen für fehlende Patches auf der Seite 'Dashboard anzeigen' auf der Start-Registerkarte. Es wird nur jeweils eine Zeile zurückgegeben.	
Parameter	Typ	Zweck
@groupName	varchar	Rechnergruppenname. Verwenden Sie Null oder eine leere Zeichenfolge für alle Gruppen.
@skipSubGroups	tinyint	Wenn im obigen Parameter ein Gruppenname bereitgestellt wird, bestimmt dieser, ob die Ergebnisse nur für die eine angegebene Gruppe oder für die angegebene Gruppe und alle ihre Untergruppen gefiltert werden sollen: 0 = Angegebene Gruppe und alle ihre Untergruppen verwenden 1 = Untergruppen weglassen – nur die eine angegebene Gruppe verwenden
Spalte	Typ	Zweck
GroupName	varchar	Rechnergruppenname. Gibt "Alle Gruppen" zurück, wenn der Parameter @groupName Null oder eine leere Zeichengruppe ist.
WithSubgroups	varchar	YES, wenn @skipSubGroups = 0 und für "Alle Gruppen" NO, wenn @skipSubGroups = 1
FullyPatched	int	Anzahl der Rechner in der durch die Parameter festgelegten Gruppe mit allen Patches
Missing12	int	Anzahl der Rechner in der durch die Parameter festgelegten

		Gruppe, bei denen 1-2 Patches fehlen
Missing35	int	Anzahl der Rechner in der durch die Parameter festgelegten Gruppe, bei denen 3-5 Patches fehlen
MissingMore5	int	Anzahl der Rechner in der durch die Parameter festgelegten Gruppe, bei denen 5 oder mehr Patches fehlen
Unscanned	int	Anzahl der Rechner in der durch die Parameter festgelegten Gruppe, die nicht gescannt wurden
Unsupported	int	Anzahl der Rechner in der durch die Parameter festgelegten Gruppe, für die Patching nicht unterstützt wird

Beispiele

Ersetzten Sie in den nachfolgenden Beispielen `machinegroup` durch den Namen der Rechnergruppe, die Sie verwenden. Wenn eine Rechnergruppe nicht aufgeführt ist, werden Daten für `Alle Gruppen` zurückgegeben.

```
SELECT FROM * fnMissingPatchCounts_UsePolicy('',0)
SELECT FROM * fnMissingPatchCounts_UsePolicy('machinegroup',0)
SELECT FROM * fnMissingPatchCounts_NoPolicy('',0)
SELECT FROM * fnMissingPatchCounts_NoPolicy('machinegroup',0)
```

fnOSCounts

fnOSCounts	Gibt die Berichtssystemtypen und deren Anzahl für die angegebene Rechnergruppe zurück. Tabellendaten gemäß Anzeige in den Betriebssystem-Kreisdiagrammen in den Executive-Übersichtsberichten und auf der Seite 'Dashboard anzeigen' auf der Start-Registerkarte. Gibt eine Zeile für jeden Betriebssystemtyp zurück.	
Parameter	Typ	Zweck
@groupName	varchar	Rechnergruppenname. Verwenden Sie Null oder eine leere Zeichenfolge für alle Gruppen.
@skipSubGroups	tinyint	Wenn im obigen Parameter ein Gruppenname bereitgestellt wird, bestimmt dieser, ob die Ergebnisse nur für die eine angegebene Gruppe oder für die angegebene Gruppe und alle ihre Untergruppen gefiltert werden sollen: 0 = Angegebene Gruppe und alle ihre Untergruppen verwenden 1 = Untergruppen weglassen – nur die eine angegebene Gruppe verwenden
Spalte	Typ	Zweck
OSType	varchar	Betriebssystemtyp, wie z. B. "Win XP", Win Vista" oder "Mac OS X"
OSCount	int	Anzahl der Betriebssystemtypen in der durch die Parameter festgelegten Gruppe

vAddRemoveList

vAddRemoveList	Von der letzten Inventarisierung zurückgegebene Anwendungsliste hinzufügen/entfernen	
Spaltenname	Typ	Zweck

Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann die Rechnergruppe, der der Rechner zugewiesen ist
applicationName	varchar(260), null	Anwendungsname aus der Hinzufügen/Entfernen-Programmliste

vAdminNotesLog

vAdminNotesLog	Anmerkungen, die jeder Administrator manuell für einen Rechner oder eine Gruppe von Rechnern eingibt. Die Einträge in diesem Protokoll verfallen nie.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
AdminLogin	varchar(100), not null	Admin-Anmeldename. (Hinweis: nicht zu verwechseln mit 'not name'; dies ist die Spalte adminName)
EventTime	datetime(3), not null	Zeitstempel-Zeichenfolge, die angibt, wann die Aktion stattgefunden hat. Standardwert ist CURRENT_TIMESTAMP, sodass hier nichts eingegeben werden muss.
NoteDesc	varchar(2000), not null	Beschreibung der Aktion

vAgentConfiguration

vAgentConfiguration	Protokoll aller Meldungen, die per E-Mail versendet wurden. Mehrere Zeilen pro Rechner.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), not null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
firstCheckin	datetime(3), null	Zeitstempel der erstmaligen Anmeldung dieses Agents beim System
lastCheckin	datetime(3), null	Zeitstempel der letzten Anmeldung dieses Agents beim System

currentUser	varchar(100), null	Anmeldename des gegenwärtig angemeldeten Benutzers. Leer, falls gegenwärtig niemand angemeldet ist
lastLoginName	varchar(100), not null	Anmeldename des letzten Benutzers, der sich bei diesem System angemeldet hat
workgroupDomainType	tinyint(3), not null	0 (oder Null) = unbekannt 1 = mit keinem verbunden 2 = Mitglied der Arbeitsgruppe 3 = Mitglied der Domain 4 = Domain-Controller
workgroupDomainName	nvarchar(32), null	Der Name der Arbeitsgruppe oder Domain
lastReboot	datetime(3), null	Zeitstempel des letzten Neustarts dieses Systems
agentVersion	int(10), null	Versionsnummer des auf diesem System installierten Agents
contactName	varchar(100), null	Der diesem Agent zugewiesene Benutzerkontaktname
contactEmail	varchar(100), null	Die diesem Agent zugewiesene Benutzer-Telefonnummer
contactPhone	varchar(100), null	Die diesem Agent zugewiesene Kontakttelefonnummer
contactNotes	varchar(1000), null	Mit den Kontaktinformationen für diesen Agent verknüpfte Anmerkungen
enableTickets	int(10), not null	0, falls dieser Benutzer keinen Zugriff auf Ticketing über die Benutzeroberfläche besitzt
enableRemoteControl	int(10), not null	0, falls dieser Benutzer keinen Zugriff auf Fernsteuerung über die Benutzeroberfläche besitzt
enableChat	int(10), not null	0, falls dieser Benutzer keinen Zugriff auf Chat über die Benutzeroberfläche besitzt
loginName	varchar(100), not null	Der diesem Benutzer zugewiesene Anmeldename (falls zutreffend), der für den Zugriff auf die Portaloberfläche des Systembenutzers benötigt wird
credentialName	varchar(100), not null	Der Benutzername der für diesen Agent eingerichteten Anmeldedaten (falls zutreffend)
primaryKServer	varchar(111), null	Adresse:Port, zu dem der Agent eine Verbindung für seine primäre Kaseya Server-Verbindung herstellt
secondaryKServer	varchar(111), null	Adresse:Port, zu dem der Agent eine Verbindung für seine sekundäre Kaseya Server-Verbindung herstellt
quickCheckinSecs	int(10), null	Intervall in Sekunden zwischen Schnell-Check-ins
agentTempDir	varchar(200), null	Das vom Agent auf diesem System verwendete Arbeitsverzeichnis

vAgentLabel

vAgentLabel	Gibt den Status der Agents an. Wird für Anzeigezwecke verwendet.	
Spaltenname	Typ	Zweck
displayName	varchar(201), null	Der Name der Rechner-ID/Gruppen-ID
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit

		verknüpften Gruppen-ID.
agentGuid	numeric(26,0), not null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
agentGuidStr	varchar(26), null	Eine Zeichenfolgenversion der agentGuid. Manche Sprachen konvertieren große Zahlen in Exponentialnotation. Die Zeichenfolgenkonvertierung verhindert dies.
online	int(10), null	0 -> offline 1 -> online 2 -> online und Benutzer hat seit mindestens 10 Minuten die Maus oder Tastatur nicht benutzt. 198 -> Konto ausgesetzt 199 -> Agent hat noch nie eingecheckt (Vorlagenkonto)
transitionTime	datetime(3), null	Wird angewendet, wenn online auf 0 oder 2 eingestellt ist. • Wenn online gleich 0, gibt dies die Zeit an, zu der der Agent zuletzt eingecheckt hat. • Wenn online gleich 2, gibt dies die Zeit an, zu der der Rechner als im Leerlauf erachtet wurde (10 Minuten nach der letzten Maus- oder Tastaturaktivität).
timezoneOffset	int(10), null	Der Zeitzonen-Offset des Agents verglichen mit der Greenwich-Zeit
currentLogin	varchar(100), null	Der Anmeldename des aktuellen Benutzers
toolTipNotes	varchar(1000), not null	Der für eine Rechner-ID angezeigte Tooltip-Text
showToolTip	tinyint(3), not null	0 -> Keine Tooltips für Rechner-ID anzeigen 1 -> Tooltips für Rechner-ID anzeigen
agntTyp	int(10), not null	0 -> Windows-Agent 4 -> Mac-Agent 5 -> Linux-Agent
agentOnlineStatus	int(10), null	

vAlertLog

vAlertLog	Protokoll aller Meldungen, die per E-Mail versendet wurden. Mehrere Zeilen pro Rechner.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann die Rechnergruppe, der der Rechner zugewiesen ist
EventTime	datetime(3), null	Zeit, zu der das Ereignis aufgezeichnet wurde
AlertEmail	varchar(1000), null	E-Mail-Adresse, an die die Meldung gesendet wird

AlertType	int(10), null	Meldungen sind einer der verschiedenen **Monitortypen** *(siehe 623)* auf. 1 – Adminkonto deaktiviert 2 – Meldung 'Dateiänderung abrufen' 3 – Neuer Agent hat das erste Mal eingecheckt 4 – Anwendung installiert oder gelöscht 5 – Agent-Verfahrensfehler festgestellt 6 – Fehler in NT-Ereignisprotokoll festgestellt 7 – Kaseya Server beendet 8 – Schutzverletzung festgestellt 9 – PCI-Konfiguration geändert 10 – Festplattenlaufwerkskonfiguration geändert 11 – RAM-Größe geändert 12 – Test-E-Mail von serverInfo.asp gesendet 13 – Geplanter Bericht abgeschlossen 14 – LAN-Watch-Meldungstyp 15 – Agent offline 16 – Festplattenspeicher niedrig 17 – Remote Control deaktiviert 18 – Agent online 19 – Neues Patch gefunden 20 – Patch-Pfad fehlt 21 – Patch-Installation fehlgeschlagen 23 – Backup-Meldung
EmailSubject	varchar(500), null	Betreffzeile der E-Mail-Nachricht
EmailBody	varchar(4000), null	E-Mail-Textkörper

vBackupLog

vBackupLog	Protokoll aller Meldungen, die per E-Mail versendet wurden. Mehrere Zeilen pro Rechner.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann die Rechnergruppe, der der Rechner zugewiesen ist
EventTime	datetime(3), null	Zeit, zu der das Ereignis aufgezeichnet wurde
description	varchar(1000), null	Beschreibung der gemeldeten Aufgabe
durationSec	int(10), null	Anzahl Sekunden, die für den Abschluss der gemeldeten Aufgabe benötigt wurde

statusType	int(10), null	0: Vollständige Datenträgersicherung 1: Offsite-Replizierung (veraltet) 2: Inkrementelle Datenträgersicherung 3: Offsite-Replizierung ausgesetzt (veraltet) 4: Offsite-Replizierung ausgelassen, weil Sicherung fehlgeschlagen (veraltet) 5: Vollständige Ordnersicherung 6: Offsite-Ordner ausgesetzt (veraltet) 7: Differentielle Datenträgersicherung 8: Inkrementelle Ordnersicherung 9: Differentielle Ordnersicherung 10: Datenträgerbestätigung 11: Ordnerbestätigung 12: Datenträgersicherung ausgelassen, weil Rechner offline ist 13: Ordnersicherung ausgelassen, weil Rechner offline ist 14: Zur Information 15: Diff od. Ink als vollst. ausgeführt, weil letzt. vollst. Datenträger nicht gefunden 16: Diff od. Ink als vollst. ausgeführt, weil letzt. vollst. Ordner nicht gefunden 17: Volume-Backup abgebrochen 18: Ordner-Backup abgebrochen 19: Volume-Abbild-Konvertierung (in KBU 3.0) 20: vollständiges synthetisches Volume-Backup (in KBU 3.0) 21: vollständiges synthetisches Ordner-Backup (in KBU 3.0)
result	int(10), null	0: Fehlschlag 1: Erfolg 2: Archivierung unvollständig
imageSize	float(53), not null	Die Größe der Sicherung

vBaseApplicationInfo / vCurrApplicationInfo

vBaseApplicationInfo vCurrApplicationInfo	Inventarisierungsergebnisse für die installierten Anwendungen. Ein Eintrag pro installierter Anwendung im Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\App Paths gefunden.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
ProductName	varchar(128), null	Produktname (z. B. Microsoft Office 2000)
ProductVersion	varchar(50),	Version (z. B. 9.0.3822)

	null	
ApplicationName	varchar(128), null	Anwendungsname (z. B. Winword.exe)
manufacturer	varchar(128), null	Herstellername (z. B. Microsoft Corporation)
ApplicationDesc	varchar(512), null	Beschreibung (z. B. Microsoft Word für Windows)
LastModifiedDate	varchar(50), null	Dateidatum (z. B. 24. 12. 2000 17:23:44)
ApplicationSize	int(10), null	Dateigröße in Byte (z. B. 8810548)
DirectoryPath	varchar(256), null	Verzeichnispfad oder Client-Desktop (z. B. C:\PROGRA~1\MICROS~4\OFFICE)

vBaseCpuInfo / vCurrCpuInfo

vBaseCpuInfo vCurrCpuInfo	Inventarisierungsergebnisse für die CPU auf einem Client-Desktoprechner. Ein Eintrag pro Inventarisierung eines Client-Desktops.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
CpuDesc	varchar(80), null	Beschreibung der CPU (z. B. Pentium III Model 8)
CpuSpeed	int(10), null	CPU-Geschwindigkeit in MHz (z. B. 601)
CpuCount	int(10), null	Anzahl der Prozessoren (z. B. 1)
TotalRam	int(10), null	Betrag des RAM in MByte (z. B. 250)

vBaseDiskInfo / vCurrDiskInfo

vBaseDiskInfo vCurrDiskInfo	Inventarisierungsergebnisse für die logischen Platten auf einem Client-Desktoprechner. Ein Eintrag pro logischer Platte von der Inventarisierung eines Client-Desktops.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername

groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
DriveLetter	varchar(100), null	Laufwerksbuchstabe der logischen Festplatte (z. B. C)
TotalSpace	int(10), null	Gesamtfestplattenkapazität in MByte (z. B. 28609 für 28.609 GB). Kann Null sein, falls nicht verfügbar.
UsedSpace	int(10), null	Belegter Festplattenspeicher in MByte (z. B. 21406 für 21.406 GB). Kann Null sein, falls nicht verfügbar.
FreeSpace	int(10), null	Freier Festplattenspeicher in MByte (z. B. 21406 für 21.406 GB). Kann Null sein, falls nicht verfügbar.
DriveType	varchar(40), null	Fixed = Festplatte Removable = Diskette oder andere Wechselmedien CDROM Network = zugeordnetes Netzwerklaufwerk
VolumeName	varchar(100), null	Dem Datenträger zugewiesener Name
FormatType	varchar(16), null	NTFS, FAT32, CDFS usw.

vBaseDriveManufacturer / vCurrDriveManufacturer

vBaseDriveManufacturer vCurrDriveManufacturer	Hardware-Audit-Ergebnisse für den Hersteller und die Produktinformationen der IDE- und SCSI-Laufwerke auf dem Client-Desktop. Ein Eintrag pro Laufwerk von der Inventarisierung eines Client-Desktops.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26,0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
DriveManufacturer	varchar(100), null	Herstellername (max. 8 Zeichen für die Daten)
DriveProductName	varchar(100), null	Produktidentifikation (max. 16 Zeichen für die Daten)
DriveProductRevision	varchar(40), null	Produktrevision (max. 4 Zeichen für die Daten)
DriveType	varchar(9), not null	Typ des gefundenen Festpattenlaufwerks

vBasePciInfo / vCurrPciInfo

vBasePciInfo vCurrPciInfo	Hardware-Inventarisierungsergebnisse für den Hersteller und die Produktinformationen der PCI-Karten auf dem Client-Desktop. Ein Eintrag pro PCI-Karte von der Inventarisierung eines Client-Desktops.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.

agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
VendorName	varchar(200), null	PCI-Herstellername
ProductName	varchar(200), null	PCI-Produktname
ProductRevision	int(10), null	Produktrevision
PciBaseClass	int(10), null	PCI-Basis-Klassennummer
PciSubClass	int(10), null	PCI-Unterklassennummer
PciBusNumber	int(10), null	PCI-Busnummer
PciSlotNumber	int(10), null	PCI-Steckplatznummer

vBasePrinterInfo / vCurrPrinterInfo

vBasePrinterInfo vCurrPrinterInfo	Druckerinventarisierungsergebnisse für die Drucker, die für den aktuellen Benutzer gefunden wurden, der bei einem Client-Desktop angemeldet ist. Ein Eintrag pro Drucker von der Inventarisierung eines Client-Desktops. Wenn kein Benutzer angemeldet ist, inventarisiert der Agent die Drucker für das Systemkonto, in der Regel den Benutzer.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
PrinterName	varchar(100), null	Name des Druckers. Der gleiche Name, der auch im Druckerkonfigurationsfenster der Systemsteuerung angezeigt wird
PortName	varchar(100), null	Name des Ports, an den der Drucker angeschlossen ist. Der gleiche Name, der auch im Druckerkonfigurationsfenster der Systemsteuerung angezeigt wird
PrinterModel	varchar(100), null	Der Modellname ist der von den Druckerinformationen abgerufene Treibername.

vCollectionMember

vCollectionMember	Listet alle Obergruppen auf, denen eine Rechner-ID angehört (falls zutreffend).	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201)	Eine verkettete Darstellung der Rechner-ID und der damit

	, null	verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), not null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100) , null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100) , null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
collectionName	varchar(100) , not null	Sammlungsname

vConfigLog

vConfigLog	Protokoll aller Konfigurationsänderungen. Nur ein Eintrag pro Änderung.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201) , null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100) , null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100) , null	Der für jeden Agent verwendete Gruppenname
EventTime	datetime(3), null	Zeitstempel-Zeichenfolge, die angibt, wann die Änderung eingegeben wurde. (Hinweis: Der Zeitstempeltyp wurde gewählt, damit alle Zeiten in der Datenbank im Format Jahr-Monat-Tag-hr-min-sec im numerischen Format angegeben werden, unabhängig von dem im SQL-Befehl gesendeten Format. Auf diese Weise können alle Datensätze beim Abrufen leicht nach der Uhrzeit sortiert werden.)
ConfigDesc	varchar(1000), null	Beschreibung der Änderung

vEventDetail

vEventDetail	Liefert eine Beschreibung eines Ereignisses.	
Spaltenname	Typ	Zweck
Partitions-ID	numeric(26,0), not null	Tenant-Identifikator
EventTypeDesc	varchar(256), not null	Beschreibung
IntervalTypeDesc	varchar(50), not null	Intervalltyp-ID
EventDesc	varchar(256), not null	Beschreibung
EventEndpoint	varchar(770), not null	Der zu sendende Endpunktname

Daten	varchar(-1), null	Datennutzlast
DataFileSpec	varchar(200), null	Weiterzugebender Dateipfad (falls vorhanden)
EffectiveDate	datetime(3), not null	Datum, an dem das Ereignis erstmalig aufgetreten ist
ExpirationDate	datetime(3), null	Ablaufdatum (falls vorhanden)
IntervalIncrement	int(10), null	Inkrement (Ganzzahl)
CreateOwnerCalendarEntries	bit, null	Boolesch, je nachdem, ob Instanzen für ein Jahr im Voraus erstellt werden oder nicht
NotifyOwnerOnStartAndCompletion	bit, not null	Boolesche Benachrichtigungsmarkierung (künftige Verwendung)
NotifySubscribersOnCompletion	bit, not null	Boolesche Benachrichtigungsmarkierung (künftige Verwendung)
OwnerUserName	varchar(50), null	Benutzername
OwnerCoveredPassword	varchar(50), null	Geschütztes Kennwort (künftige Verwendung)
StartNotificationNote	varchar(100), null	Benachrichtigungshinweis (künftige Verwendung)
CompletionNotificationNote	varchar(100), null	Fertigstellungshinweis (künftige Verwendung)
SuspenseIntervalTypeID	int(10), null	Typ des Fälligkeitsintervalls, wie in der Intervalltyp-ID-Tabelle angegeben
SuspenseIntervalIncrement	int(10), null	Fälligkeitsintervall-Inkrement
SuspenseExpirationEventID	int(10), null	Ereignis, das nach Ablauf des Fälligkeitstermins gesendet werden soll (künftige Verwendung)
SuspenseExpirationNote	varchar(100), null	Hinweis zum Fälligkeitsablauf (künftige Verwendung)
ErrorEventID	int(10), null	Ereignis, das bei Auftreten eines Fehlers gesendet werden soll (künftige Verwendung)
ErrorNote	varchar(100), null	Fehlerhinweis (künftige Verwendung)
PreparationEventID	int(10), null	(künftige Verwendung)
PreparationEventData	varchar(200), null	(künftige Verwendung)
CalendarEntriesAllowed	bit, not null	Angabe, ob jährliche Instanzenerstellung zulässig ist
DefaultEventEndpoint	varchar(770), not null	Standard-Endpunktname
OwnerNotificationAllowed	bit, not null	Benachrichtigung für Eigentümer
SubscriberNotificationAllowed	bit, not null	Benachrichtigung für Abonnent (was ist ein Abonnent)
SysMinIncrement	int(10), not null	Anzahl der Ausführungen (wie viele Male)
SysMaxIncrement	int(10), not null	Wiederholung in Sekunden
MinIncrement	int(10), not null	Minimales Inkrement
MaxIncrement	int(10), not null	Maximales Inkrement
EventId	int(10), not null	Eindeutige Ereignistyp-ID
Aktiv	bit, not null	Ist aktiv
RunCount	int(10), null	Anzahl der Ausführungen (wie viele Male)
ScriptId	int(10), null	Mit Agent-Verfahren verknüpfte Skript-ID
AgentGuid	numeric(26,0), null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
orgCalendarScheduleId	numeric(26,0), null	Im Organisationskalender-Plan zugeordnete ID

vEventInstanceDetail

vEventInstanceDetail	Liefert eine Beschreibung einer ausgelösten Ereignisinstanz.	
Spaltenname	Typ	Zweck
Partitions-ID	numeric(26,0), not null	Tenant-Identifikator
ScheduledDate	datetime(3), not null	Datum/Uhrzeit, zu der die Instanz geplant wurde
StartedDate	datetime(3), null	Datum/Uhrzeit, zu der die Ausführung der Instanz begonnen wurde
CompletedDate	datetime(3), null	Datum/Uhrzeit, zu der die Ausführung der Instanz abgeschlossen wurde
InProcess	bit, not null	Das Ereignis wird gerade ausgeführt
CompletedWithErrors	bit, not null	Mit Fehlern abgeschlossen
EventTypeDesc	varchar(256), not null	Beschreibung
IntervalTypeDesc	varchar(50), not null	Intervalltyp-ID
EventDesc	varchar(256), not null	Beschreibung
EventEndpoint	varchar(770), not null	Der zu sendende Endpunktname
Daten	varchar(-1), null	Datennutzlast
DataFileSpec	varchar(200), null	Weiterzugebender Dateipfad (falls vorhanden)
EffectiveDate	datetime(3), not null	Datum, an dem das Ereignis erstmalig aufgetreten ist
ExpirationDate	datetime(3), null	Ablaufdatum (falls vorhanden)
IntervalIncrement	int(10), null	Inkrement (Ganzzahl)
CreateOwnerCalendarEntries	bit, null	Boolesch, je nachdem, ob Instanzen für ein Jahr im Voraus erstellt werden oder nicht
NotifyOwnerOnStartAndCompletion	bit, not null	Boolesche Benachrichtigungsmarkierung (künftige Verwendung)
NotifySubscribersOnCompletion	bit, not null	Boolesche Benachrichtigungsmarkierung (künftige Verwendung)
OwnerUserName	varchar(50), null	Benutzername
OwnerCoveredPassword	varchar(50), null	Geschütztes Kennwort (künftige Verwendung)
StartNotificationNote	varchar(100), null	Benachrichtigungshinweis (künftige Verwendung)
CompletionNotificationNote	varchar(100), null	Fertigstellungshinweis (künftige Verwendung)
SuspenseIntervalTypeID	int(10), null	Typ des Fälligkeitsintervalls, wie in der Intervalltyp-ID-Tabelle angegeben
SuspenseIntervalIncrement	int(10), null	Fälligkeitsintervall-Inkrement
SuspenseExpirationEventID	int(10), null	Ereignis, das nach Ablauf des Fälligkeitstermins gesendet werden soll (künftige Verwendung)
SuspenseExpirationNote	varchar(100), null	Hinweis zum Fälligkeitsablauf (künftige Verwendung)
ErrorEventID	int(10), null	Ereignis, das bei Auftreten eines Fehlers gesendet werden soll (künftige Verwendung)

ErrorNote	varchar(100), null	Fehlerhinweis (künftige Verwendung)
PreparationEventID	int(10), null	(künftige Verwendung)
PreparationEventData	varchar(200), null	(künftige Verwendung)
EventInstanceID	numeric(18,0), not null	Eindeutige Ereignisinstanz-ID
SuspenseDate	datetime(3), null	Fälligkeitsdatum eines Ereignisses
CalendarEntriesAllowed	bit, not null	Angabe, ob jährliche Instanzenerstellung zulässig ist
DefaultEventEndpoint	varchar(770), not null	Standard-Endpunktname
OwnerNotificationAllowed	bit, not null	Benachrichtigung für Eigentümer
SubscriberNotificationAllowed	bit, not null	Benachrichtigung für Abonnent
SysMinIncrement	int(10), not null	Minimales Inkrement
SysMaxIncrement	int(10), not null	Maximales Inkrement
EventId	int(10), not null	Eindeutige Ereignistyp-ID
Aktiv	bit, not null	Ist aktiv
ErrorMessage	varchar(500), null	Fehlermeldung (falls zutreffend)
InstanceData	varchar(-1), null	Datennutzlast
ConfiguredRunCount	int(10), null	Anzahl der Ausführungen (wie viele Male)
CurrentRunCount	int(10), null	Anzahl der Ausführungen (wie viele Male)
InstanceRunCount	int(10), null	Anzahl der Ausführungen (wie viele Male)
ScriptId	int(10), null	Mit Agent-Verfahren verknüpfte Skript-ID
AgentGuid	numeric(26,0), null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
powerUpIfOffline	char(1), null	Bei 'Wahr' ist der Rechner hochgefahren
skipIfOffline	char(1), null	Bei 'Wahr' wird der Rechner übersprungen, wenn er offline ist
runAfterNextReboot	char(1), null	Bei 'Wahr' beginnt die Ausführung nach Neustart
orgCalendarScheduleId	numeric(26,0), null	Im Organisationskalender-Plan zugeordnete ID

vEventInstanceHistoryDetail

vEventInstanceHistoryDetail	Liefert einen Verlauf von ausgelösten Ereignisinstanzen.	
Spaltenname	Typ	Zweck
Partitions-ID	numeric(26,0), null	Tenant-Identifikator
ScheduledDate	datetime(3), null	Datum/Uhrzeit, zu der die Instanz geplant wurde
StartedDate	datetime(3), null	Datum/Uhrzeit, zu der die Ausführung der Instanz begonnen wurde
CompletedDate	datetime(3), null	Datum/Uhrzeit, zu der die Ausführung der Instanz abgeschlossen wurde
InProcess	int(10), not null	Das Ereignis wird gerade ausgeführt
CompletedWithErrors	bit, null	Mit Fehlern abgeschlossen
EventTypeDesc	varchar(256), not null	Beschreibung

IntervalTypeDesc	varchar(50), not null	Intervalltyp-ID
EventDesc	varchar(256), not null	Beschreibung
EventEndpoint	varchar(770), not null	Der zu sendende Endpunktname
Daten	varchar(-1), null	Datennutzlast
DataFileSpec	varchar(200), null	Weiterzugebender Dateipfad (falls vorhanden)
EffectiveDate	datetime(3), not null	Datum, an dem das Ereignis erstmalig aufgetreten ist
ExpirationDate	datetime(3), null	Ablaufdatum (falls vorhanden)
IntervalIncrement	int(10), null	Inkrement (Ganzzahl)
CreateOwnerCalendarEntries	bit, null	Boolesch, je nachdem, ob Instanzen für ein Jahr im Voraus erstellt werden oder nicht
NotifyOwnerOnStartAndCompletion	bit, not null	Boolesche Benachrichtigungsmarkierung (künftige Verwendung)
NotifySubscribersOnCompletion	bit, not null	Boolesche Benachrichtigungsmarkierung (künftige Verwendung)
OwnerUserName	varchar(50), null	Benutzername
OwnerCoveredPassword	varchar(50), null	Geschütztes Kennwort (künftige Verwendung)
StartNotificationNote	varchar(100), null	Benachrichtigungshinweis (künftige Verwendung)
CompletionNotificationNote	varchar(100), null	Fertigstellungshinweis (künftige Verwendung)
SuspenseIntervalTypeID	int(10), null	Typ des Fälligkeitsintervalls, wie in der Intervalltyp-ID-Tabelle angegeben
SuspenseIntervalIncrement	int(10), null	Fälligkeitsintervall-Inkrement
SuspenseExpirationEventID	int(10), null	Ereignis, das nach Ablauf des Fälligkeitstermins gesendet werden soll (künftige Verwendung)
SuspenseExpirationNote	varchar(100), null	Hinweis zum Fälligkeitsablauf (künftige Verwendung)
ErrorEventID	int(10), null	Ereignis, das bei Auftreten eines Fehlers gesendet werden soll (künftige Verwendung)
ErrorNote	varchar(100), null	Fehlerhinweis (künftige Verwendung)
PreparationEventID	int(10), null	(künftige Verwendung)
PreparationEventData	varchar(200), null	(künftige Verwendung)
EventInstanceID	numeric(18,0), null	Eindeutige Ereignisinstanz-ID
SuspenseDate	datetime(3), null	Fälligkeitsdatum eines Ereignisses
CalendarEntriesAllowed	bit, not null	Angabe, ob jährliche Instanzenerstellung zulässig ist
DefaultEventEndpoint	varchar(770), not null	Standard-Endpunktname
OwnerNotificationAllowed	bit, not null	Benachrichtigung für Eigentümer
SubscriberNotificationAllowed	bit, not null	Benachrichtigung für Abonnent
SysMinIncrement	int(10), not null	Minimales Inkrement
SysMaxIncrement	int(10), not null	Maximales Inkrement
EventId	int(10), not null	Eindeutige Ereignistyp-ID
Aktiv	bit, not null	Ist aktiv
ErrorMessage	varchar(500), null	Fehlermeldung (falls zutreffend)
InstanceData	varchar(-1), null	Datennutzlast
ConfiguredRunCount	int(10), null	Anzahl der Ausführungen (wie viele Male)

CurrentRunCount	int(10), null	Anzahl der Ausführungen (wie viele Male)
InstanceRunCount	int(10), null	Anzahl der Ausführungen (wie viele Male)
ScriptId	int(10), null	Mit Agent-Verfahren verknüpfte Skript-ID
AgentGuid	numeric(26,0), null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
orgCalendarScheduleId	numeric(26,0), null	Im Organisationskalender-Plan zugeordnete ID

vLicenseInfo

vLicenseInfo	Während der Inventarisierung erfasste Lizenzinformationen	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
computerName	varchar(80), null	Der im Betriebssystem gefundene Computername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
Publisher	varchar(100), null	Software-Publisher (für gewöhnlich der Publisher-Registrierungswert)
ProductName	varchar(100), null	Softwaretitel (für gewöhnlich der DisplayName-Wert, es kann jedoch auch der Titel des Registrierungsschlüssels verwendet werden)
LicenseCode	varchar(100), null	Lizenzcode (für gewöhnlich der ProductID-Wert)
ProductKey	varchar(100), null	Produktschlüssel
LicenseVersion	varchar(100), null	Vom Scanner zurückgegebene Versionszeichenfolge (falls zutreffend)
InstallDate	varchar(100), null	Vom Scanner zurückgegebene Installationsdatumszeichenfolge (falls zutreffend)
OperatingSystem	varchar(16), null	Betriebssystem des Computers
OperatingSystemVersion	varchar(150), null	Betriebssystemversion
loginName	varchar(100), null	Aktuell angemeldeter Benutzer
lastLoginName	varchar(100), null	Zuvor angemeldeter Benutzer

vMachine

vMachine	Die über jeden Client-Desktoprechner bekannten Informationen

Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26,0), not null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der vollständige Rechnername. Der Rechnername besteht aus allen Zeichen links vom Dezimalkomma.
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
Manufacturer	varchar(100), null	Herstellerzeichenfolge (Typ 1)
ProductName	varchar(100), null	Produktnamenzeichenfolge (Typ 1)
MachineVersion	varchar(100), null	Versionszeichenfolge (Typ 1)
SysSerialNumber	varchar(100), null	Seriennummernzeichenfolge (Typ 1)
ChassisSerialNumber	varchar(100), null	Seriennummer des Gehäuses (Typ 3)
ChassisAssetTag	varchar(100), null	Bestandsetikettnummer des Gehäuses (Typ 3)
BusSpeed	varchar(100), null	Geschwindigkeit des externen Bus (in MHz) (Typ 4)
MaxMemorySize	varchar(100), null	Maximale Speichermodulgröße (in MB) (Typ 16 - Maximale Kapazität oder, falls Typ 16 nicht verfügbar ist, Maximale Speichermodulgröße Typ 5)
MaxMemorySlots	varchar(100), null	Anzahl der verknüpften Speicherslots (Anzahl der Speichergeräte in Typ 16 oder, falls Typ 16 nicht verfügbar ist, Anzahl der verknüpften Speicherslots in Typ 5)
ChassisManufacturer	varchar(100), null	Gehäusehersteller (Typ 3)
ChassisType	varchar(100), null	Gehäusetyp (Typ 3)
ChassisVersion	varchar(100), null	Gehäuseversion (Typ 3)
MotherboardManufacturer	varchar(100), null	Hersteller der Hauptplatine (Typ 2)
MotherboardProductCode	varchar(100), null	Produktcode der Hauptplatine (Typ 2)
MotherboardVersion	varchar(100), null	Version der Hauptplatine (Typ 2)
MotherboardSerialNumber	varchar(100), null	Seriennummer der Hauptplatine (Typ 2)
ComputerName	varchar(80), null	Der im Betriebssystem gefundene Computername
IpAddress	varchar(20), null	IP-Adresse des Computers in a.b.c.d-Notation
SubnetMask	varchar(20), null	Subnetzmaske in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DefaultGateway	varchar(20), null	Standard-Gateway-IP-Adresse in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.

DnsServer1	varchar(20), null	IP-Adresse von DNS-Server #1 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DnsServer2	varchar(20), null	IP-Adresse von DNS-Server #2 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DnsServer3	varchar(20), null	IP-Adresse von DNS-Server #3 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DnsServer4	varchar(20), null	IP-Adresse von DNS-Server #4 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DhcpEnabled	int(10), null	0 -> Daten nicht verfügbar 1 -> DHCP auf Client-Computer ist aktiviert 2 -> Deaktiviert
DhcpServer	varchar(20), null	IP-Adresse des DHCP-Servers in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
WinsEnabled	int(10), null	0 -> Daten nicht verfügbar 1 -> WINS-Auflösung auf Client-Computer ist aktiviert 2 -> Deaktiviert
PrimaryWinsServer	varchar(20), null	IP-Adresse des primären WINS-Servers in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
SecondaryWinsServer	varchar(20), null	IP-Adresse des sekundären WINS-Servers in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
ConnectionGatewayIp	varchar(20), null	IP-Adresse in a.b.c.d-Notation, die vom Kaseya Server als Quelladresse des Agent ermittelt wurde. Diese IP ist das Netzwerk-Gateway des Agents. Sie unterscheidet sich von der IP-Adresse, falls sich der Computer beispielsweise hinter NAT befindet. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
ipv6Address	varchar(40), null	Die ipv6-Adresse. Null, wenn keine Adresse angegeben wird.
OsType	varchar(8), null	Zeichenfolge enthält den Typ des Betriebssystems, z. B. NT4, 2000, NT3.51 oder WIN32s. Wird aus Teilen der MajorVersion, MinorVersion und PlatformId abgeleitet.
OsInfo	varchar(150), null	Zeichenfolge enthält zusätzliche Informationen zum Betriebssystem, wie z. B. Build 1381 Service Pack 3. Wird aus Teilen der BuildNumber und CsdVersion abgeleitet.
MajorVersion	int(10), null	Hauptversionsnummer aus einen GetVersionEx() Windows-Funktionsaufruf abgeleitet.
MinorVersion	int(10), null	Nebenversionsnummer aus einem GetVersionEx() Windows-Funktionsaufruf abgeleitet. Falls die PlatformId Win32 für Windows lautet, so weist die MinorVersion 0 auf Windows 95 hin. Lautet die PlatformId Win32 für Windows, so weist eine MinorVersion > 0 auf Windows 98 hin.
MacAddr	varchar(40), null	Zeichenfolge, die die physikalische Adresse, d. h. die Media Access Control-Adresse, der Verbindung angibt. Eine MAC-Adresse ist folgendermaßen aufgebaut: 00-03- 47-12-65-77
LoginName	varchar(100), null	Benutzername des gegenwärtig angemeldeten Benutzers. Dieser Wert wird bei jedem Schnell-Check-in aktualisiert. Die Fehlerprotokolldatei des Agents wird bei jeder Änderung aktualisiert.
timezoneOffset	int(10), not null	Der Zeitzonen-Offset des Agents verglichen mit der Greenwich-Zeit
agentInstGuid	varchar(40), not null	Der eindeutige Teil des Pfads zum Agent-Verzeichnis des K2 (Version 6.0.0.0 und höher) und zum Dienstnamen als KA+vMachine.agentInstGuid.

vMonitorAlarmAlert

vMonitorAlarmAlert	Liste aller durch Monitormeldungen erstellten Alarme	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineName	varchar(100), null	Der für jeden Agent verwendete Rechnername
GroupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
MonitorAlarmID	int(10), not null	Eindeutige Monitoralarmnummer
MonitorType	tinyint(3), not null	4 -> Monitormeldung
EventLogType	int(10), null	Nur anwendbar für AlertType=6 (NT-Ereignisprotokoll) 0 -> Anwendungsereignisprotokoll 1 -> Systemereignisprotokoll 2 -> Systemereignisprotokoll
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trend
AlertType	int(10), not null	Meldungen sind einer der verschiedenen **Monitortypen** *(siehe 623)* auf. 1 – Adminkonto deaktiviert 2 – Meldung 'Dateiänderung abrufen' 3 – Neuer Agent hat das erste Mal eingecheckt 4 – Anwendung installiert oder gelöscht 5 – Agent-Verfahrensfehler festgestellt 6 – Fehler in NT-Ereignisprotokoll festgestellt 7 – Kaseya Server beendet 8 – Schutzverletzung festgestellt 9 – PCI-Konfiguration geändert 10 – Festplattenlaufwerkskonfiguration geändert 11 – RAM-Größe geändert 12 – Test-E-Mail von serverInfo.asp gesendet 13 – Geplanter Bericht abgeschlossen 14 – LAN-Watch-Meldungstyp 15 – Agent offline 16 – Festplattenspeicher niedrig 17 – Remote Control deaktiviert 18 – Agent online 19 – Neues Patch gefunden 20 – Patch-Pfad fehlt 21 – Patch-Installation fehlgeschlagen 23 – Backup-Meldung
Message	varchar(3000), null	Aus Alarm erstellte Nachricht, Textkörper einer E-Mail-Nachricht
AlarmSubject	varchar(500), null	Betreff des Alarms bzw. der E-Mail-Nachricht
AlarmEmail	varchar(1000), null	E-Mail-Adresse(n), an die der Alarm gesendet wird

EventTime	datetime(3), not null	Datum und Uhrzeit des Alarms
TicketID	varchar(30), null	Die aus dem erstellte Ticket-ID
MonitorAlarmState	smallint(5), null	0 -> Beendet 1 -> Wird ausgeführt
AdminName	varchar(100), null	Benutzer, der dem Rechner die Monitormeldung zugewiesen hat

vMonitorAlarmCounter

vMonitorAlarmCounter	Liste aller durch Monitorzähler erstellten Alarme	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineName	varchar(100), null	Der für jeden Agent verwendete Rechnername
GroupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
MonitorAlarmID	int(10), not null	Eindeutige Monitoralarmnummer
MonitorType	tinyint(3), not null	0 -> Monitorzähler
MonitorName	varchar(100), not null	Name des Monitorzählerobjekts
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trend
Message	varchar(3000), null	Aus Alarm erstellte Nachricht, Textkörper einer E-Mail-Nachricht
AlarmSubject	varchar(500), null	Betreff des Alarms bzw. der E-Mail-Nachricht
AlarmEmail	varchar(1000), null	E-Mail-Adresse(n), an die der Alarm gesendet wird
EventTime	datetime(3), not null	Datum und Uhrzeit des Alarms
TicketID	varchar(30), null	Die aus dem erstellte Ticket-ID
LogValue	float(53), null	Wert, der den Alarm auslöst
MonitorAlarmState	smallint(5), null	0 -> Beendet 1 -> Wird ausgeführt
AdminName	varchar(100), null	Benutzer, der dem Rechner den Monitorzähler zugewiesen hat

vMonitorAlarmProcess

vMonitorAlarmProcess	Liste aller durch Monitorprozesse erstellten Alarme	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineName	varchar(100), null	Der für jeden Agent verwendete Rechnername
GroupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
MonitorAlarmID	int(10), not null	Eindeutige Monitoralarmnummer
MonitorType	tinyint(3), not null	2 -> Monitorprozess
MonitorName	varchar(100), not null	Name des Monitorprozessobjekts
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trend
Message	varchar(3000), null	Aus Alarm erstellte Nachricht, Textkörper einer E-Mail-Nachricht
AlarmSubject	varchar(500), null	Betreff des Alarms bzw. der E-Mail-Nachricht
AlarmEmail	varchar(1000), null	E-Mail-Adresse(n), an die der Alarm gesendet wird
EventTime	datetime(3), not null	Datum und Uhrzeit des Alarms
TicketID	varchar(30), null	Die aus dem erstellte Ticket-ID
LogValue	float(53), null	Wert, der den Alarm auslöst. Nachstehend sind die Prozesswerte aufgelistet:
MonitorAlarmState	smallint(5), null	0 -> Beendet 1 -> Wird ausgeführt
AdminName	varchar(100), null	Benutzername des Administrators

vMonitorAlarmService

vMonitorAlarmService	Liste aller durch Monitordienste erstellten Alarme	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.

MachineName	varchar(100), null	Der für jeden Agent verwendete Rechnername
GroupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
MonitorAlarmID	int(10), not null	Eindeutige Monitoralarmnummer
MonitorType	tinyint(3), not null	0 -> Monitordienst
MonitorName	varchar(100), not null	Name des Monitordienstobjekts
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trend
Message	varchar(3000), null	Aus Alarm erstellte Nachricht, Textkörper einer E-Mail-Nachricht
AlarmSubject	varchar(500), null	Betreff des Alarms bzw. der E-Mail-Nachricht
AlarmEmail	varchar(1000), null	E-Mail-Adresse(n), an die der Alarm gesendet wird
EventTime	datetime(3), not null	Datum und Uhrzeit des Alarms
TicketID	varchar(30), null	Die aus dem erstellte Ticket-ID
LogValue	float(53), null	Wert, der den Alarm auslöst. Nachstehend sind die Dienstwerte aufgelistet: -1 -> Existiert nicht 0 -> Reserviert 1 -> Beendet 2 -> Start ausstehend 3 -> Beenden ausstehend 4 -> Wird ausgeführt 5 -> Fortsetzen ausstehend 6 -> Pause ausstehend 7 -> Angehalten
MonitorAlarmState	smallint(5), null	0 -> Beendet 1 -> Wird ausgeführt
AdminName	varchar(100), null	Benutzer, der dem Rechner den Monitordienst zugewiesen hat

vMonitorAlarmSNMP

vMonitorAlarmSNMP	Liste aller durch Monitor-SNMP-Abrufobjekte erstellten Alarme	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	numeric(26,0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineName	varchar(100), null	Der für jeden Agent verwendete Rechnername

GroupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
MonitorAlarmID	int(10), not null	Eindeutige Monitoralarmnummer
MonitorType	tinyint(3), not null	3 -> Monitor-SNMP-Abruf
MonitorName	varchar(100), not null	Name des SNMP-Abrufobjekts
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trend
Message	varchar(3000), null	Aus Alarm erstellte Nachricht, Textkörper einer E-Mail-Nachricht
AlarmSubject	varchar(500), null	Betreff des Alarms bzw. der E-Mail-Nachricht
AlarmEmail	varchar(1000), null	E-Mail-Adresse(n), an die der Alarm gesendet wird
EventTime	datetime(3), not null	Datum und Uhrzeit des Alarms
TicketID	varchar(30), null	Die aus dem erstellte Ticket-ID
LogValue	float(53), null	Wert, der den Alarm auslöst. Falls der Rückgabewert des SNMP-Abrufobjekt-Befehls eine Zeichenfolge ist, ist der Wert diese Nachricht
SNMPName	varchar(50), null	Der vom SNMP-Gerät beim Scan zurückgegebene Wert
SNMPCustomName	nvarchar(100), null	Benutzerspezifischer Name des SNMP-Geräts
MonitorAlarmState	smallint(5), null	0 -> Beendet 1 -> Wird ausgeführt
AdminName	varchar(100), null	Benutzer, der dem Rechner den Monitor-SNMP-Abruf zugewiesen hat

vMonitorAlarmSystemCheck

vMonitorAlarmSystemCheck	Liste aller durch Monitorsystemprüfungen erstellten Alarme	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	numeric(26,0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineName	varchar(100), null	Der für jeden Agent verwendete Rechnername
GroupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
MonitorAlarmID	int(10), not null	Eindeutige Monitoralarmnummer
MonitorType	tinyint(3), not	5 -> Monitorsystemprüfung

	null	
SystemCheckType	int(10), null	1 -> Webserver 2 -> DNS-Server 4 -> Portverbindung 5 -> Ping 6 -> Benutzerdefiniert
AlarmType	smallint(5), null	0 -> Alarm 1 -> Trend
Parameter1	varchar(1000), null	Erster bei der Systemprüfung verwendeter Parameter
Parameter2	varchar(1000), null	(Optional) Zweiter bei der Systemprüfung verwendeter Parameter
Message	varchar(3000), null	Aus Alarm erstellte Nachricht, Textkörper einer E-Mail-Nachricht
AlertSubject	varchar(500), null	Betreff des Alarms bzw. der E-Mail-Nachricht
AlarmEmail	varchar(1000), null	E-Mail-Adresse(n), an die der Alarm gesendet wird
EventTime	datetime(3), not null	Datum und Uhrzeit des Alarms
TicketID	varchar(30), null	Die aus dem erstellte Ticket-ID
MonitorAlarmState	smallint(5), null	0 -> Beendet 1 -> Wird ausgeführt
AdminName	varchar(100), null	Benutzer, der dem Rechner den Monitorzähler zugewiesen hat

vNetStatsLog

vNetStatsLog	Protokoll der Netzwerkstatistiken vom Agent	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
EventTime	datetime(3), null	Zeitstempel-Zeichenfolge, die angibt, wann die Änderung eingegeben wurde. (Hinweis: Der Zeitstempeltyp wurde gewählt, damit alle Zeiten in der Datenbank im Format Jahr-Monat-Tag-hr-min-sec im numerischen Format angegeben werden, unabhängig von dem im SQL-Befehl gesendeten Format. Auf diese Weise können alle Datensätze beim Abrufen leicht nach der Uhrzeit sortiert werden.)
BytesRcvd	int(10), null	Anzahl der während dieser Statistikperiode empfangenen Byte
BytesSent	int(10), null	Anzahl der während dieser Statistikperiode gesendeten Byte

ApplicationName	varchar(800), null	Name der Anwendung, die das Netzwerk verwendet

vNtEventLog

vNtEventLog	Ereignisprotokolldaten, die von jedem verwalteten Rechner erfasst wurden	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
logType	int(10), null	1 -> Anwendungsprotokoll 2 -> Sicherheitsprotokoll 3 -> Systemprotokoll
eventType	int(10), null	1 -> Fehler 2 -> Warnung 4 -> Zur Information 8 -> Erfolgs-Audit 16 -> Fehler-Audit
eventTime	datetime(3), null	Zeit, zu der das Ereignis stattfand
ApplicationName	nvarchar(200), null	Quelle des Ereignisprotokolls
EventCategory	nvarchar(200), null	Ereignisprotokollkategorie
eventId	int(10), null	Ereignis-ID des Ereignisprotokolls
username	nvarchar(200), null	Ereignisprotokollbenutzer
computerName	nvarchar(200), null	Computername des Ereignisprotokolls
EventMessage	nvarchar(2000), null	Ereignisprotokollmeldung

vOnBoardDeviceInfo

vOnBoardDeviceInfo	Von KaSmBios.exe während einer Inventarisierung von Informationen zu integrierten Geräten erfasste Daten. Eine Zeile pro aktivem Steckplatz. Alle Informationen werden von Typ 10 abgerufen.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.

agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
DeviceType	varchar(100), null	Gerätetyp
DeviceDesc	varchar(100), null	Gerätebeschreibung

vPatchApprovalPolicyStatus

vPatchApprovalPolicyStatus	Der Patch-Bestätigungsstatus eines Patch nach Patch-Richtlinie.	
Spaltenname	Typ	Zweck
UpdateClassificationCode	smallint(5), not null	Update-Klassifizierung: 100 -> Sicherheits-Update (Kritisch) 101 -> Sicherheits-Update (Wichtig) 102 -> Sicherheits-Update (Mittel) 103 -> Sicherheits-Update (Niedrig) 104 -> Sicherheits-Update (Nicht eingestuft) 110 -> Kritisches Update 120 -> Update-Rollup 200 -> Service Pack 210 -> Update 220 -> Feature Pack 230 -> Tool 900 -> Nicht klassifiziert 999 -> Kaseya-Patch-Test
UpdateClassification	varchar(43), not null	Wie UpdateClassification im Zeichenfolgenformat
Bestätigt	int(10), null	Anzahl der Patch-Richtlinien, in denen dieses Patch bestätigt wurde
Abgelehnt	int(10), null	Anzahl der Patch-Richtlinien, in denen dieses Patch abgelehnt wurde
Noch offen	int(10), null	Anzahl der Patch-Richtlinien, in denen dieses Patch aussteht
Gesamtsummen	int(10), null	Gesamtanzahl der Patch-Richtlinien, in denen dieses Patch bestätigt, abgelehnt oder ausstehend ist
Produkt	varchar(300), null	Produkt, dem dieses Patch zugeordnet ist
Richtlinie	varchar(100), null	Name der Patch-Richtlinie
UpdateClassificationDefaultApprovalCode	smallint(5), not null	0 – Bestätigt 1 – Abgelehnt 2 – Ausstehend
UpdateClassificationDefaultApproval	varchar(8), not null	Bestätigt, ausstehend oder abgelehnt
ProductDefaultApprovalCode	smallint(5), not null	0 – Bestätigt 1 – Abgelehnt

		2 – Ausstehend
ProductDefaultApproval	varchar(8), not null	Bestätigt, ausstehend oder abgelehnt
PartitionID	numeric(26,0), not null	Tenant-Identifikator (siehe partnerPartition-Tabelle)

vPatchApprovalStatus

vPatchApprovalStatus	Zeigt den Bestätigungsstatus eines Patch. Eine Zeile pro aktivem Patch.	
Spaltenname	Typ	Zweck
patchDataId	int(10), not null	Eindeutiger Identifikator für dieses Patch innerhalb der Datenbank
KBArticle	varchar(12), not null	Microsoft Knowledge Base-Artikelnummer
SecurityBulletin	varchar(40), not null	Microsoft Sicherheitsberichtsnummer
Title	varchar(250), not null	Patch-Titel
UpdateClassificationId	smallint(5), not null	Numerische Darstellung der Patch-Update-Klassifizierung. Wird zur Vereinfachung der Filterung eingeschlossen. Mögliche Werte: 100 = Kritisches Sicherheits-Update (Hohe Priorität) 101 = Wichtiges Sicherheits-Update (Hohe Priorität) 102 = Mittleres Sicherheits-Update (Hohe Priorität) 103 = Niedriges Sicherheits-Update (Hohe Priorität) 104 = Nicht eingestuftes Sicherheits-Update (Hohe Priorität) 110 = Kritisches Update (Hohe Priorität) 120 = Update-Rollup (Hohe Priorität) 200 = Service Pack (Optional) 210 = Update (Optional) 220 = Feature Pack (Optional) 230 = Tool (Optional)
UpdateClassification	varchar(43), not null	Textdarstellung der Patch-Update-Klassifizierung
Product	varchar(300), null	Produkt, dem dieses Patch zugeordnet ist
PublishedDate	datetime(3), null	Datum, an dem dieses Patch zuletzt von Microsoft aktualisiert wurde, falls verfügbar
Language	varchar(30), not null	Sprachunterstützung für dieses Patch
numApproved	int(10), null	Anzahl der Patch-Richtlinien, in denen dieses Patch bestätigt wurde
numDenied	int(10), null	Anzahl der Patch-Richtlinien, in denen dieses Patch abgelehnt wurde
numPending	int(10), null	Anzahl der Patch-Richtlinien, in denen die Bestätigung für dieses Patch aussteht
InstallationWarning	varchar(27), not null	Gibt 'Nur manuelle Installation', 'Nur Windows-Aktualisierung', 'Nur Produktaufrüstung' oder eine leere Zeichenfolge zurück.
PartitionID	numeric(26, 0), not null	Der eindeutige Bezeichner einer Tenant-Partition für einen gemeinsam genutzten Kaseya Server und eine Datenbank.

vPatchConfiguration

vPatchConfiguration	Gibt die verschiedenen Konfigurationen für das Patch an. Eine Zeile pro Rechner.	
Spaltenname	Typ	Zweck
agentGuid	numeric(26, 0), not null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineID	varchar(201), null	Der Rechnername, die Rechnergruppe und die Organisation, die einem Rechner zugewiesen wurden
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
MachineName	varchar(80), null	Der für jeden Agent verwendete Rechnername
ComputerName	varchar(80), null	Der im Betriebssystem gefundene Computername
ReverseGroupName	varchar(100), null	Rechnergruppe, dann die Organisation, der der Rechner zugewiesen ist
GroupName	varchar(100), not null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
OperatingSystem	varchar(16), null	Betriebssystem des Computers
OSInformation	varchar(150), null	Betriebssysteminformationen
CurrentUser	varchar(100), null	Derzeit angemeldeter Benutzer
LastLoggedOnUser	varchar(100), null	Zuvor angemeldeter Benutzer
PatchScanTypeSetting	int(10), not null	Typ des Patch-Scans: -1 = Betriebssystem nicht für Patch-Scans unterstützt 0 = Alter Patch-Scan 1 = WUA-Patch-Scan (32-Bit) 2 = WUA-Patch-Scan (64-Bit)
PatchScanType	varchar(300), null	Typ der Patch-Scan-Beschreibung:
RebootSetting	int(10), not null	Neustartaktion nach Patch-Installation: 0 = Sofortiger Neustart 1 = Anfrage – Nichts tun, falls der Benutzer nicht in <RebootWarnMinutes> Minuten antwortet 2 = Kein Neustart nach Aktualisierung. Falls vorhanden, E-Mail an <RebootWarningEmailAddress< senden 3 = Anfrage – Neustart, falls der Benutzer nicht in <RebootWarnMinutes> Minuten antwortet 4 = Benutzer warnen, dass der Rechner in <RebootWarnMinutes> Minuten neu startet 5 = Neustart übergehen, falls der Benutzer angemeldet ist 6 = Neustart am <RebootDay> um <RebootTime> nach der Installation 7 = Anfrage zum Neustart alle <RebootWarnMinutes> Minuten
RebootAction	varchar(143), null	Beschreibung der Neustartaktion nach Patch-Installation:

PreRebootScript	varchar(260), not null	Skript-ID des Skripts, das sofort vor dem Neustart-Schritt im Patch-Neustart-Skript ausgeführt werden soll
PostRebootScript	varchar(260), not null	Skript-ID des Skripts, das sofort nach dem Patch-Neustart ausgeführt werden soll (aus scriptAssignmentReboot)
RebootWarnMinutes	int(10), null	Warnzeit in Minuten für RebootSetting 1,3,4,7
RebootDay	int(10), null	Tag, an dem Patch-Neustart für RebootSetting 6 erzwungen werden soll: 0 = Jeden Tag 1 = Sonntag 2 = Montag 3 = Dienstag 4 = Mittwoch 5 = Donnerstag 6 = Freitag 7 = Samstag
RebootTime	varchar(10), null	Zeit, zu der Patch-Neustart für RebootSetting 6 erzwungen werden soll:
RebootWarningEmailAddress	varchar(100), null	E-Mail-Adresse, an die eine E-Mail-Nachricht für einen Neustart nach einer Patch-Installation für RebootSetting 2 gesendet werden soll
FileSourceSetting	int(10), not null	Quelle der Patch-Installationsdatei: 0 = Vom Internet 1 = Vom Systemserver 2 = Vom Dateiserver
FileSourceConfig	varchar(169), not null	Beschreibung der Quelle der Patch-Installationsdatei
UseAgentTempDirOnDriveMostFreeSpace	int(10), not null	Ziel der heruntergeladenen Patch-Datei: 0 = Vom Agent konfiguriertes Arbeitslaufwerk/-verzeichnis verwenden 1 = Vom Agent konfiguriertes Arbeitsverzeichnis auf lokalem Laufwerk verwenden, das den meisten freien Speicherplatz hat
DeleteAfterInstall	int(10), not null	Heruntergeladene Patch-Datei nach der Installation löschen: 0 = Nicht löschen 1 = Löschen
FileSourceMachineId	varchar(201), null	Rechnergruppen-ID des Dateiservers für FileSourceSetting 2
FileSourceUNCPath	varchar(300), null	UNC-Pfad des Dateiservers für FileSourceSetting 2
FileSourceLocalPath	varchar(300), null	Lokaler Rechnerpfad des Dateiservers für FileSourceSetting 2
LanCacheName	varchar(200), null	Der Name des LAN-Cache
LanCacheMachineId	varchar(201), null	Die Rechner-ID des Rechners, der den LAN-Cache hostet
LanCacheUNCPath	varchar(260), null	Der UNC-Pfad zum LAN-Cache
LanCacheLocalPath	varchar(260),null	Der lokale Verzeichnispfad zum LAN-Cache
UseInternetSourceAsFallback	int(10), null	Falls Dateiserver nicht zugänglich, das Internet für FileSourceSetting 2 verwenden

WinAutoUpdateSetting	int(10), not null	Automatische Windows-Aktualisierungseinstellung 0 = Automatische Windows-Aktualisierungskonfiguration festgelegt. Kann vom Benutzer auf dem Rechner nicht geändert werden 1 = Automatische Windows-Aktualisierungskonfiguration deaktiviert. Kann vom Benutzer auf dem Rechner nicht geändert werden 2 = Benutzersteuerung
WinAutoUpdateConfig	varchar(93), null	Beschreibung der automatischen Windows-Aktualisierung

vPatchPieChartCountsNoPolicy

vPatchPieChartCountsNoPolicy	Gibt die Anzahl der Patches für Rechner ohne eine zugewiesene Richtlinie an.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
Agent-Guid	numeric(26,0), not null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
MachineId	varchar(201), null	Der für jeden Agent verwendete Rechnername
ComputerName	varchar(80), null	Der im Betriebssystem gefundene Computername
ReverseGroupName	varchar(100), null	Rechnergruppe, dann die Organisation, der der Rechner zugewiesen ist
GroupName	varchar(100), not null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
OperatingSystem	varchar(16), null	Betriebssystem des Computers
OSInformation	varchar(150), null	Betriebssysteminformationen
CurrentUser	varchar(100), null	Derzeit angemeldeter Benutzer
LastLoggedOnUser	varchar(100), null	Zuvor angemeldeter Benutzer
Kategorie	varchar(26), not null	• Nicht gescannt • Fehlende Patches: 6 oder mehr • Betriebssystem nicht unterstützt

vPatchPieChartCountsUsePolicy

vPatchPieChartCountsUsePolicy	Gibt die Anzahl der Patches für Rechner mit einer zugewiesenen Richtlinie an.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
Agent-Guid	numeric(26,0), not null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
MachineId	varchar(201), null	Der für jeden Agent verwendete Rechnername

ComputerName	varchar(80), null	Der im Betriebssystem gefundene Computername
ReverseGroupName	varchar(100), null	Rechnergruppe, dann die Organisation, der der Rechner zugewiesen ist
GroupName	varchar(100), not null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
OperatingSystem	varchar(16), null	Betriebssystem des Computers
OSInformation	varchar(150), null	Betriebssysteminformationen
CurrentUser	varchar(100), null	Derzeit angemeldeter Benutzer
LastLoggedOnUser	varchar(100), null	Zuvor angemeldeter Benutzer
Kategorie	varchar(26), not null	Nicht gescannt Fehlende Patches: 6 oder mehr Betriebssystem nicht unterstützt

vPatchPolicy

vPatchPolicy	Zeigt den Bestätigungsstatus eines Patch. Eine Zeile pro aktivem Patch in jeder Patch-Richtlinie.	
Spaltenname	Typ	Zweck
patchDataId	int(10), not null	Eindeutiger Identifikator für dieses Patch innerhalb der Datenbank
Policy	varchar(100), null	Name der Patch-Richtlinie
KBArticle	varchar(12), not null	Microsoft Knowledge Base-Artikelnummer
SecurityBulletin	varchar(40), not null	Microsoft Sicherheitsberichtsnummer
Title	varchar(250), not null	Patch-Titel
UpdateClassificationId	smallint(5), not null	Numerische Darstellung der Patch-Update-Klassifizierung. Wird zur Vereinfachung der Filterung eingeschlossen. Mögliche Werte: 100 = Kritisches Sicherheits-Update (Hohe Priorität) 101 = Wichtiges Sicherheits-Update (Hohe Priorität) 102 = Mittleres Sicherheits-Update (Hohe Priorität) 103 = Niedriges Sicherheits-Update (Hohe Priorität) 104 = Nicht eingestuftes Sicherheits-Update (Hohe Priorität) 110 = Kritisches Update (Hohe Priorität) 120 = Update-Rollup (Hohe Priorität) 200 = Service Pack (Optional) 210 = Update (Optional) 220 = Feature Pack (Optional) 230 = Tool (Optional)
UpdateClassification	varchar(43), not null	Textdarstellung der Patch-Update-Klassifizierung
Product	varchar(300), null	Produkt, dem dieses Patch zugeordnet ist
PublishedDate	datetime(3), null	Datum, an dem dieses Patch zuletzt von Microsoft aktualisiert wurde, falls verfügbar

Language	varchar(30), not null	Sprachunterstützung für dieses Patch
ApprovalStatusId	smallint(5), not null	Numerische Darstellung des Patch-Bestätigungsstatus. Wird zur Vereinfachung der Filterung eingeschlossen. Mögliche Werte: 0 = Bestätigt 1 = Abgelehnt 2 = Bestätigung ausstehend
ApprovalStatus	varchar(16), not null	Textdarstellung des Patch-Bestätigungsstatus
Admin	varchar(100), not null	Name des Benutzers, der die letzte Statusänderung vorgenommen hat ("*System*" weist darauf hin, dass der Bestätigungsstatus basierend auf dem standardmäßigen Bestätigungsstatus der Patch-Richtlinie vom System oder aber durch 'KB überschreiben' festgelegt wurde)
Changed	datetime(3), not null	Zeitstempel der letzten Änderung des Bestätigungsstatus
InstallationWarning	varchar(20), not null	Gibt 'Nur manuelle Installation', 'Nur Windows-Aktualisierung', 'Nur Produktaufrüstung' oder eine leere Zeichenfolge zurück.
StatusNotes	varchar(500), not null	Anmerkungen, die vom Administrator zum Patch-Bestätigungsstatus hinzugefügt wurden
PartitionID	numeric(26, 0), not null	Der eindeutige Bezeichner einer Tenant-Partition für einen gemeinsam genutzten Kaseya Server und eine Datenbank.

vPatchPolicyMember

vPatchPolicyMember	Listet alle Patch-Richtlinien auf, denen die einzelnen Rechner-IDs angehören, falls zutreffend.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	numeric(26, 0), not null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineID	varchar(201), null	Der für jeden Agent verwendete Rechnername
ComputerName	varchar(80), null	Der im Betriebssystem gefundene Computername
ReverseGroupName	varchar(100), null	Rechnergruppe, dann die Organisation, der der Rechner zugewiesen ist
GroupName	varchar(100), not null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
OperatingSystem	varchar(16), null	Betriebssystem des Computers
OSInformation	varchar(150), null	Betriebssysteminformationen
CurrentUser	varchar(100), null	Derzeit angemeldeter Benutzer
LastLoggedOnUser	varchar(100), null	Zuvor angemeldeter Benutzer

PolicyName	varchar(100), not null	Name der Patch-Richtlinie

vPatchStatus

vPatchStatus	Zeigt den Status aller Patches auf Rechnerbasis. Eine Zeile pro Rechner.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), not null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
MachineId	varchar(201), null	Der für jeden Agent verwendete Rechnername
ComputerName	varchar(80), null	Der im Betriebssystem gefundene Computername
ReverseGroupName	varchar(100), null	Rechnergruppe, dann die Organisation, der der Rechner zugewiesen ist
GroupName	varchar(100), not null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
OperatingSystem	varchar(16), null	Betriebssystem des Computers
OSInformation	varchar(150), null	Betriebssysteminformationen
CurrentUser	varchar(100), null	Derzeit angemeldeter Benutzer
LastLoggedOnUser	varchar(100), null	Zuvor angemeldeter Benutzer
KBArticle	varchar(10), not null	Vom Patch-Scanner angegebene Microsoft KB-Artikelnummer
SecurityBulletin	varchar(40), not null	Vom Patch-Scanner angegebene Berichts-ID-Zeichenfolge
Title	varchar(250), not null	Titel des Updates
Product	varchar(300), not null	Produkt, dem dieses Patch zugeordnet ist
Language	varchar(30), null	Sprache des Produkts

UpdateClassification	smallint(5), not null	Update-Klassifizierung: 100 -> Sicherheits-Update (Kritisch) 101 -> Sicherheits-Update (Wichtig) 102 -> Sicherheits-Update (Mittel) 103 -> Sicherheits-Update (Niedrig) 104 -> Sicherheits-Update (Nicht eingestuft) 110 -> Kritisches Update 120 -> Update-Rollup 200 -> Service Pack 210 -> Update 220 -> Feature Pack 230 -> Tool 900 -> Nicht klassifiziert 999 -> Kaseya-Patch-Test
UpdateClassificationDescription	varchar(43), not null	Wie UpdateClassification im Zeichenfolgenformat
ReleaseDate	datetime(3), null	Freigabedatum des Patch
ApprovalStatus	smallint(5), not null	0 -> bestätigt 1 -> nicht bestätigt 2 -> Bestätigung ausstehend
ApprovalStatusDescription	varchar(16), not null	Wie ApprovalStatus im Zeichenfolgenformat
InstallSeparate	tinyint(3), not null	0 -> Dieses Patch kann zusammen mit anderen Patches installiert werden. 1 -> Dieses Patch muss getrennt von anderen Patches installiert werden (eigener Neustart erforderlich).
IsSuperseded	tinyint(3), not null	0 -> Update wurde nicht abgelöst 1 -> Update wurde von einem späteren Update abgelöst
PatchAppliedFlag	int(10), not null	0 -> Patch wurde nicht angewendet 1 -> Patch wurde angewendet
PatchStatus	int(10), not null	0 -> Installation dieses Patch nicht geplant 1 -> Installation dieses Patch planen Flags, mit denen alle Patches zu einem einzigen Skript gebündelt werden. Festlegen, wenn Installationsskripts generiert werden. 2 -> Patch-Installation fehlgeschlagen, keine Meldung gesendet 3 -> Patch-Installation fehlgeschlagen, Meldung gesendet 4 -> Patch installiert. Warten auf Neustart zur erneuten Bestätigung 5 -> Rollback für dieses Patch planen 6 -> '/install-as-user'-Patch nicht installiert; Benutzer ist nicht angemeldet 7 -> Office-Patch nicht installiert; Benutzeranforderung zur Installation wurde abgelehnt oder ist abgelaufen 8 -> Patch abrufen/installieren fehlgeschlagen; Client-Anmeldedaten sind ungültig
PatchStatusDescription	varchar(42), not null	Wie PatchStatus im Zeichenfolgenformat
PendingManualInstall	int(10), not null	Patch durch manuelle Aktualisierung ausgewählt (Rechner-Update oder Patch-Update): 0 -> nicht für Installation ausgewählt 1 -> für Installation ausgewählt

PatchIgnoreFlag	int(10), not null	0 -> dieses Patch verarbeiten 1 -> dieses Patch ignorieren
InstallationWarning	varchar(22), not null	Gibt 'Nur manuelle Installation', 'Nur Windows-Aktualisierung', 'Nur Produktaufrüstung', 'Internet-basierte Installation' oder eine leere Zeichenfolge zurück.
InstallDate	datetime(3), null	Zeitstempel der Anwendung dieses Patch durch den VSA
InstalledBy	varchar(100), null	Name des Administrators (falls wir das Patch installiert haben) oder der Wert aus der Registrierung (falls der Scanner den Wert zurückgegeben hat)
Description	varchar(1500), null	Patch-Beschreibung
UninstallNotes	varchar(1500), null	Anmerkungen für das Patch deinstallieren
patchDataId	int, not null	Schlüssel zur patchData-Tabelle

vPatchStatusByAgent

vPatchStatusByAgent	Beschreibt den Patch-Status eines einzelnen Agent-Rechners.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
Agent-Guid	numeric(26,0), not null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
MachineId	varchar(201), null	Der für jeden Agent verwendete Rechnername
ComputerName	varchar(80), null	Der im Betriebssystem gefundene Computername
ReverseGroupName	varchar(100), null	Rechnergruppe, dann die Organisation, der der Rechner zugewiesen ist
GroupName	varchar(100), not null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
OperatingSystem	varchar(16), null	Betriebssystem des Computers
OSInformation	varchar(150), null	Betriebssysteminformationen
CurrentUser	varchar(100), null	Derzeit angemeldeter Benutzer
LastLoggedOnUser	varchar(100), null	Zuvor angemeldeter Benutzer
LastCheckinTime	datetime(3), not null	Datum/Uhrzeit des letzten Check-ins durch den Agent
LastRebootTime	datetime(3), null	Datum/Uhrzeit des letzten Neustarts durch den Agent
totalPatches	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der Patches
installed	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der installierten Patches
missingApproved	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der fehlenden bestätigten Patches
missingDenied	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der fehlenden abgelehnten/ignorierten Patches
missingManual	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der fehlenden

		bestätigten Patches, die manuell installiert werden müssen
anstehend	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der Patches, deren Installation aussteht
notReady	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der Patches, für deren Installation der Benutzer angemeldet sein musste und die Bedingung nicht erfüllt wurde
schlug fehl	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der Patches, deren Installation fehlgeschlagen ist
rebootPending	int(10), not null	Die für agentGuid gemeldete Gesamtanzahl der Patches, deren endgültiger Status erst nach dem nächsten Neustart festgestellt werden kann
initialUpdateRunning	int(10), not null	Bei 'Wahr' wird das erste Update ausgeführt.
testStatus	int(10), null	Diese Markierung gibt an, ob die aktuellen Patch-Einstellungen für diesen Benutzer getestet wurden oder nicht. Jedes Mal, wenn der Quellpfad des Patches oder die Benutzeranmeldedaten geändert werden, wird diese Markierung zurückgesetzt. -2 – Test ausstehend -1,null – nicht getestet 0 – Test erfolgreich >0 – Test fehlgeschlagen, wobei bit 0 für einen Registrierungstest-Fehler und bit 1 für einen Dateitest-Fehler festgelegt sind (für die Anmeldeinformationen bestehen möglicherweise keine Administratorrechte) 1 – Patch-Test fehlgeschlagen (Registrierung) 2 – Patch-Test fehlgeschlagen (Datei) 4 – Patch-Test fehlgeschlagen (Registrierung und Datei) else – Patch-Datei konnte nicht installiert werden 10000 – keine ausführbare Datei heruntergeladen 10001 – Patch konnte nicht vom LAN-Server kopiert werden 10002 – Fehler bei lokalen Anmeldeinformationen 10003 – Fehler – fehlende Anmeldeinformationen für Netzwerk 10004 – ungültige Netzwerkanmeldedaten oder LAN-Server war nicht verfügbar 10005 – Die Dateiquellkonfiguration für diesen Rechner ist ungültig. 10006 – ungültige LAN-Cache-Konfiguration oder LAN-Cache war nicht verfügbar 61440 – Die ausführbare Datei wurde heruntergeladen, aber nicht ausgeführt. Die Anmeldeinformationen sind möglicherweise ungültig.
testStatusDescription	varchar(89), not null	Beschreibung des oben Genannten.
lastScanType	smallint(5), not null	Typ des letzten Patch-Scans: 0 -> Alter Scan 1 -> WUA-Scan (online) 3 -> WUA-Offline-Scan (WSUSSCN2.CAB) 4 -> Macintosh-Scan
lastScanTypeDescription	varchar(12), not null	Beschreibung des oben Genannten.
scanStatus	varchar(20), not null	Nicht gescannt Patch-Scan erfolgreich Unbestimmt
nonSupportedOS	varchar(300), not	Null, wenn das Betriebssystem des Rechners die Anwendung

	null	von Patches unterstützt. Wert des Betriebssystemelement von patchscn.xml, wenn das Betriebssystem die Anwendung von Patches nicht unterstützt.
lastPatchScan	datetime(3), null	Datum/Uhrzeit des letzten Patch-Scan
nextPatchScan	datetime(3), null	Datum/Uhrzeit des nächsten geplanten Patch-Scan
patchScanRecurrenceLabel	nvarchar(512), not null	
patchScanRecurrenceDetailsLabel	nvarchar(512), not null	
patchScanExcludeTimeRangeLabel	nvarchar(512), not null	
patchScanRecurrenceEndLabel	nvarchar(512), not null	
patchScanOfflineLabel	nvarchar(256), not null	
lastAutomaticUpdate	datetime(3), null	Datum/Uhrzeit des letzten automatischen Updates
nextAutomaticUpdate	datetime(3), null	Datum/Uhrzeit des nächsten geplanten automatischen Updates
autoUpdateRecurrenceLabel	nvarchar(512), not null	
autoUpdateRecurrenceDetailsLabel	nvarchar(512), not null	
autoUpdateExcludeTimeRangeLabel	nvarchar(512), not null	
autoUpdateRecurrenceEndLabel	nvarchar(512), not null	
autoUpdateOfflineLabel	nvarchar(256), not null	
wuaSelfUpdateRequired	tinyint(3), not null	Selbstupdate des WUA-Clients: 0 – Unbekannt 1 – Erforderlich 2 – NICHT erforderlich
wuaSelfUpdateRequiredDescription	varchar(12), not null	Beschreibung des obigen Codes.
online	int(10), null	0 -> offline 1 -> online 2 -> online und Benutzer hat seit mindestens 10 Minuten die Maus oder Tastatur nicht benutzt. 198 -> Konto ausgesetzt 199 -> Agent hat noch nie eingecheckt (Vorlagenkonto)

vPortInfo

vPortInfo	Von KaSmBios.exe während einer Inventarisierung von Portverbinder-Informationen erfasste Daten. Eine Zeile pro aktivem Steckplatz. Alle Informationen werden von Typ 8 abgerufen.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201)	Eine verkettete Darstellung der Rechner-ID und der damit

	, null	verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100) , null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100) , null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
InternalDesc	varchar(100) , null	Interne Beschreibung
ExternalDesc	varchar(100) , null	Externe Beschreibung
ConnectionType	varchar(100) , null	Verbindungstyp
PortType	varchar(100) , null	Porttyp

vScriptLog

vScriptLog	Protokoll der Verfahrensausführungen aus Sicht des Kaseya Server	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201) , null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100) , null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100) , null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
EventTime	datetime(3), null	Zeitstempel-Zeichenfolge, die angibt, wann die Änderung eingegeben wurde. (Hinweis: Der Zeitstempeltyp wurde gewählt, damit alle Zeiten in der Datenbank im Format Jahr-Monat-Tag-hr-min-sec im numerischen Format angegeben werden, unabhängig von dem im SQL-Befehl gesendeten Format. Auf diese Weise können alle Datensätze beim Abrufen leicht nach der Uhrzeit sortiert werden.)
ScriptName	varchar(260) , null	Name des Verfahrens
ScriptDesc	varchar(100 0), null	Ereignisbeschreibung
AdminName	varchar(100) , null	Name des Administrators, der dieses Verfahren geplant hat

vScriptStatus

vScriptStatus	Verfahrensstatus für jeden Client

Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
scriptName	varchar(260), null	Name des Verfahrens
LastExecTime	datetime(3), null	Zeitstempel-Zeichenfolge, die angibt, wann das Verfahren ausgeführt wurde
lastExecStatus	varchar(1000), null	Status der letzten Ausführung. Folgende Zeichenfolgen sind möglich: Verfahrensübersicht: Erfolg <ELSE oder THEN>Verfahrensübersicht: Fehlgeschlagen <ELSE oder THEN> in # step<ELSE oder THEN>wird durch das entsprechende Wort ELSE oder THEN ersetzt. # wird durch die Anzahl der Schritte ersetzt, die in dem Verfahren fehlgeschlagen sind (nicht nützlich, es sei denn, die Verarbeitung wird auch nach einem Fehlschlag fortgesetzt). 'step' wird durch die Arbeitsschritte ersetzt, falls das Verfahren bei mehr als einem (1) Schritt fehlschlägt.
AdminLogin	varchar(100), null	Name des Administrators, der dieses Verfahren zuletzt geplant hat. (Diese Spalte nicht mit adminName benennen, da dies ein primärer Schlüssel ist, der von der Datenbankmigration verwendet wird. adminName und emailAddr sollten nicht in der gleichen Tabelle erscheinen.

vSystemInfo

vSystemInfo	Über die Funktion **Systeminformationen** *(siehe 154)* gesammelte Daten	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
Manufacturer	varchar(100), null	Systemhersteller-Zeichenfolge
Product Name	varchar(100), null	Vom Hersteller angegebener Name oder Modellnummer des Rechners
System Version	varchar(100), null	Rechnerversion-Zeichenfolge
System Serial Number	varchar(100), null	Vom Hersteller angegebene Zeichenfolge der Rechner-Seriennummer
Chassis Serial Number	varchar(100), null	Vom Hersteller angegebene Zeichenfolge der Seriennummer
Chassis Asset Tag	varchar(100)	Vom Hersteller angegebene Zeichenfolge des Bestandsetiketts

	, null	
External Bus Speed	varchar(100), null	Busgeschwindigkeit der Hauptplatine
Max Memory Size	varchar(100), null	Max. Speichergröße, für die dieses System konfiguriert werden kann
Max Memory Slots	varchar(100), null	Max. Anzahl der Speichersteckplätze dieses Systems
Chassis Manufacturer	varchar(100), null	Name des Herstellers des Gehäuses
Chassis Type	varchar(100), null	Gehäusetyp des Systems
Chassis Version	varchar(100), null	Versionszeichenfolge des Gehäuses
Motherboard Manufacturer	varchar(100), null	Name des Herstellers der Hauptplatine
Motherboard Product	varchar(100), null	Modellname der Hauptplatine
Motherboard Version	varchar(100), null	Versionsnummer der Hauptplatine
Motherboard Serial Num	varchar(100), null	Seriennummer der Hauptplatine
Processor Family	varchar(100), null	Name der Prozessorfamilie
Processor Manufacturer	varchar(100), null	Name des Prozessorherstellers
Processor Version	varchar(100), null	Versionszeichenfolge des Prozessors
CPU Max Speed	varchar(100), null	Max. Geschwindigkeit dieses Prozessors
CPU Current Speed	varchar(100), null	Konfigurierte Geschwindigkeit dieses Prozessors

* Über Audit > **Systeminformationen** *(siehe 154)* benutzerdefinierte Spalten werden in den Datenbankansicht **vSystemInfoManual** *(siehe 525)* angezeigt.

vSystemInfoManual

vSystemInfo	Der Funktion **Systeminformationen** *(siehe 154)* zugefügte benutzerdefinierte Felder und Werte	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), not null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
fieldName	nvarchar(100), not null	Der Name des benutzerdefinierten Feldes
fieldValue	varchar(100), null	Der Wert des benutzerdefinierten Feldes

vTicketField

vTicketField	Mit jedem Ticket sind eine Reihe von Feldern verknüpft. Drei dieser Felder sind Standardfelder: Status, Priorität und Kategorie. Außerdem kann eine Reihe von Benutzerfeldern hinzugefügt werden, die in dieser Ansicht angezeigt werden. Jedes Feld besitzt einen Datentyp. Alle Listen werden als Ganzzahlwerte gespeichert. Die Ansicht vTicketField enthält den verknüpften Text für jeden Listenwert.	
Spaltenname	Typ	Zweck
TicketID	int(10), null	Eindeutige Ticket-Identifikationsnummer in einer einzelnen Partition
TicketLabel	varchar(50), null	Die Feldbezeichnung
IntegerValue	int(10), null	Der Wert eines Ganzzahlfelds
NumberValue	numeric(15, 4), null	Der Wert eines numerischen Felds
StringValue	varchar(500), null	Der Wert eines Zeichenfolgenfelds
ListValue	varchar(50), null	Der Wert eines Listenfelds

vTicketNote

vTicketNote	Anmerkungen zu Trouble-Tickets werden in der Datenbank gespeichert. Zu jeder Ticket-Übersicht kann es mehrere Anmerkungen geben. Anhand eines Zeitstempels wird die Reihenfolge festgelegt, in der diese angehängt wurden.	
Spaltenname	Typ	Zweck
TicketID	int(10), null	Eindeutige ID-Nummer des Trouble-Tickets
author	varchar(100), null	Die Person, die diese Anmerkung in dem Ticket geschrieben hat
TicketNoteTime	datetime(3), not null	Zeitstempel, der angibt, wann die Anmerkung hinzugefügt wurde
TicketNote	varchar(2000), not null	Inhalt der Ticket-Anmerkung
HiddenNote	int(10), not null	0, falls die Anmerkung sichtbar ist. 1, falls die Anmerkung ausgeblendet ist.
PartitionID	numeric(26, 0), not null	Identifikator des Tenants.
CreationDate	datetime(3), null	Datum/Uhrzeit der Erstellung des Tickets
DueDate	datetime(3), null	Fälligkeitsdatum des Tickets

vTicketSummary

vTicketSummary	Übersicht über Trouble-Tickets. Eine Zeile pro Ticket. Für die Namen, die in der Ansichts-Übersichtstabelle angezeigt werden, werden Spaltennamen verwendet.	
Spaltenname	Typ	Zweck
TicketID	int(10), null	Eindeutige ID-Nummer des Trouble-Tickets
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
TicketSummary	varchar(256), not null	Ein kurze Beschreibung des Tickets
Assignee	varchar(100), null	Der Admin-Name, dem dieses Ticket zugewiesen ist
CreatedBy	varchar(100), null	Admin-Name (oder Rechner-ID, falls vom Benutzer angegeben) der Person, die das Ticket erstellt hat
CreationDate	datetime(3), null	Zeitstempel der Ticketerstellung
DueDate	datetime(3), null	Fälligkeitsdatum des Tickets
LastModifiedDate	datetime(3), null	Datum, an dem die letzte Anmerkung für dieses Ticket eingegeben wurde
ResolutionDate	datetime(3), null	Zeitstempel der Schließung des Tickets
UserName	varchar(100), null	Der Name des Absenders.
UserEmail	varchar(200), null	Die E-Mail-Adresse des Absenders
UserPhone	varchar(100), null	Die Telefonnummer des Absenders
TicketInternalId	int(10), not null	Eine interne, eindeutige Ticket-ID für alle Partitionen
PartitionID	numeric(26, 0), not null	Der eindeutige Bezeichner einer Tenant-Partition für einen gemeinsam genutzten Kaseya Server und eine Datenbank.

vUptimeHistory

vUptimeHistory	Die für den Laufzeit-Historie-Bericht erfassten Daten. Wird in Verbindung mit dem getMachUptime-Webdienst verwendet.	
Spaltenname	Typ	Zweck
Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.

Machine_GroupID	varchar(201), null	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	numeric(26, 0), null	Ein global eindeutiger Identifikator eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents
machName	varchar(100), null	Der für jeden Agent verwendete Rechnername
groupName	varchar(100), null	Organisation, dann Rechnergruppe, der der Rechner zugewiesen ist
eventTime	datetime(3), null	Zeitstempel des Anfangs des Zeitsegments
duration	int(10), null	Anzahl der Sekunden, die dieses Zeitsegment dauerte
type	int(10), null	1 – Agent ist angemeldet, kann jedoch keine Verbindung zum Kaseya Server herstellen 2 – Agent ist angemeldet und mit dem Kaseya Server verbunden 3 – Agent hat sich normal abgemeldet 4 – Anormaler Agent-Abbruch 5 – Agent-Alarme wurden ausgesetzt (die Aussetzungsdauer sollte bei der Berechnung der Gesamt-Laufzeit (Funktion 'getMachUptime') nicht berücksichtigt werden 6 – Aussetzung wurde beendet
loginName	varchar(100), null	Name des Benutzers, der während dieses Zeitsegments angemeldet war. (SYSTEM, wenn niemand angemeldet war)

vvProAssetDetails

vvProAssetDetails	Listet Informationen über einen vPro-aktivierten Rechner auf, einschließlich der Herstellerangaben zur Hauptplatine.	
Spaltenname	Typ	Zweck
agentGuid	numeric(26,0), null	26-stellige, nach Zufallsprinzip gewählte Nummer, die diesen Agent eindeutig identifiziert. Der Hauptdatensatz wird in machNameTab gespeichert.
displayName	varchar(201), null	Falls auf dem vPro-Rechner ein Agent installiert ist, ist der Anzeigename die machine.GroupId einer normalen Agent-Auflistung. Andernfalls ist er leer.
hostName	varchar(255), null	Name des Rechners im LAN
computerName	varchar(255), null	Der im Betriebssystem gefundene Computername
assetId	varchar(50), not null	Die Bestands-ID ist Teil der grundlegenden Hardwareinformationen.
computerModel	varchar(65), null	Modellbezeichnung des Computers
computerManufacturer	varchar(65), null	Hersteller des Computers
computerVersion	varchar(65), null	Versionsnummer des Computers
computerSerialNumber	varchar(65), null	Seriennummer des Computers
mbManufacturer	varchar(65), null	Hauptplatinenhersteller
mbProductName	varchar(65), null	Produktname der Hauptplatine
mbVersion	varchar(65), null	Versionsnummer der Hauptplatine
mbSerialNumber	varchar(65), null	Seriennummer der Hauptplatine
mbAssetTag	varchar(65), null	Bestandsetikett der Hauptplatine

mbReplaceable	tinyint(3), null	Wahr oder falsch, je nachdem ob die Hauptplatine austauschbar ist
biosVendor	varchar(65), null	Hersteller des BIOS
biosVersion	varchar(65), null	Versionsnummer des BIOS
biosReleaseDate	datetime(3), null	BIOS-Freigabedatum
biosSupportedFunctions	varchar(1000), null	Liste der vom BIOS unterstützten Funktionen
ipAddress	varchar(19), null	ipAddress des vPro-Rechners, die von der Energieverwaltung und beim Remote-ISO-Boot verwendet wird

Kapitel 12

API-Web-Services

In diesem Kapitel

VSA-API-Webdienst

In diesem Abschnitt

VSA-API-Webdienst – Überblick

Der VSA-**API-Webdienst** stellt eine generische Oberfläche für einen Client zur Verfügung und ermöglicht die Programmierung einer Schnittstelle zum VSA. Dank dieser API kann ein Client eine Verbindung zu einer Anwendung eines Drittanbieters herstellen. Die API konzentriert sich auf die folgenden Dienste:

- **Verbindung** – Dieser Dienst ermöglicht dem Benutzer der API, sich zu authentifizieren und eine GUID zu erhalten, die er während der gesamten Kommunikation verwenden kann. Die GUID kann auf die gleiche Weise wie auch ein Benutzer veralten.
- **Tickets** – Dieser Dienst stellt grundlegende Funktionen zur Verfügung, um den Benutzer über neue Tickets zu benachrichtigen. Mit dieser Funktion können Benutzer Felder auf einem Ticket aktualisieren.
- **Alarme** – Dieser Dienst stellt grundlegende Funktionen zur Verfügung, um den Benutzer über neue Alarme zu benachrichtigen und einen Alarm als geschlossen zu markieren.
- **Rechner** – Dieser Dienst stellt eine Anforderung zur Verfügung, eine Gruppe von Daten über einen oder mehrere Rechner zu sammeln.

Der VSA **API-Webdienst** basiert auf der **Web Services Description Language (WSDL)**. Die WSDL wird in einem Browser angezeigt und stellt eine abstrakte Beschreibung der Daten zur Verfügung, die mit einem Webdienst ausgetauscht werden können. Ein Client-Programm, das eine Verbindung zu einem Webdienst herstellt, kann über die WSDL ablesen, welche Funktionen auf dem Server zur Verfügung stehen. Eventuell verwendete spezielle Datentypen werden in der WSDL-Datei in Form eines XML-Schemas eingebettet. Der Client kann dann mithilfe des SOAP eine der auf der WSDL aufgelisteten Funktionen aufrufen.

Es folgt ein Beispiel einer vsaWS-Ausgabe:

KaseyaWS

GetMachine

Returns machine detail for the submitted Machine_GroupID.

Test

The test form is only available for requests from the local machine.

SOAP 1.1

The following is a sample SOAP 1.1 request and response. The **placeholders** shown need to be replaced with actual values.

```
POST /vsaWS/kaseyaWS.asmx HTTP/1.1
Host: 192.168.214.224
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "KaseyaWS/GetMachine"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <GetMachine xmlns="KaseyaWS">
      <req>
        <Machine_GroupID>string</Machine_GroupID>
        <SessionID>decimal</SessionID>
      </req>
    </GetMachine>
  </soap:Body>
</soap:Envelope>
```

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <soap:Body>
    <GetMachineResponse xmlns="KaseyaWS">
      <GetMachineResult>
        <Machine_GroupID>string</Machine_GroupID>
        <machName>string</machName>
        <groupName>string</groupName>
        <Manufacturer>string</Manufacturer>
        <ProductName>string</ProductName>
        <MachineVersion>string</MachineVersion>
```

VSA-API-Webdienst aktivieren

So aktivieren Sie den VSA-API-Webdienst:

- Öffnen Sie die Seite "System > **Konfigurieren** *(siehe 429)*" im VSA.
- Klicken Sie auf das Kontrollkästchen **VSA-API-Webdienst aktivieren**.
- Greifen Sie über `http://<your-KServer>/vsaWS/KaseyaWS.asmx` auf den VSA-API-Webdienst zu.

> **Hinweis:** Der **KSD-API-Webdienst** *(http://help.kaseya.com/webhelp/DE/KSD/7000000/index.asp#5761.htm)* beschreibt zusätzliche API-Operationen für **Service Desk**.

Spezielle Felder

Die folgenden Felder werden in die Antwort auf jede Anforderung eingeschlossen.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

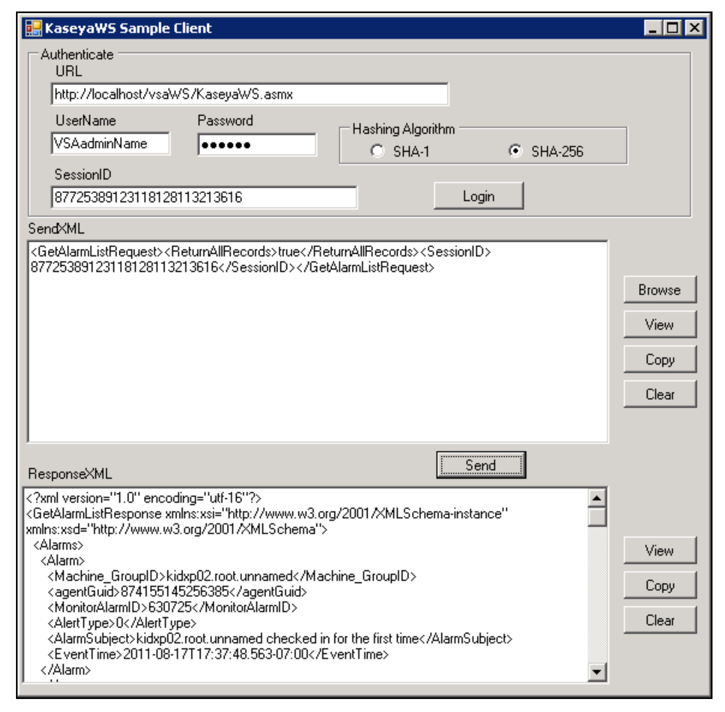
Es wird eine **Sitzungs-ID** vom Webdienst erstellt und an den Client zurückgegeben, wenn eine Methode

erstmals vom Client aufgerufen wird. Die gleiche Sitzungs-ID muss mit jeder in dieser Sitzung aufgerufenen Methode vom Client zurückgegeben werden. Die Sitzungs-ID ist nur gültig, wenn sie von der gleichen IP-Adresse erhalten wird, auf der auch die Authentifizierung stattfand.

API-Beispielanwendung für C#

Im Lieferumfang des VSA-API-Webdiensts befinden sich auch ein GUI-Testclient sowie ein Satz von Test-XML-Seiten, die Ihnen helfen, sich mit den verschiedenen API-Vorgängen vertraut zu machen. Der C#-Quellcode für die **API-Beispielanwendung für C#** wird Ihnen ohne jegliche Einschränkungen zur Verfügung gestellt. Sie können daraus ersehen, wie der Client konstruiert wurde, und auch beliebige Teile dieses Codes in Ihre eigene Anwendung integrieren.

> **Hinweis:** Eine **API-Beispielseite für ASP** *(siehe 536)* steht Ihnen ebenfalls zur Verfügung.



So führen Sie den Beispiel-Client aus:

1. Führen Sie den Beispiel-Client auf Ihrem Kaseya Server im folgenden Verzeichnis aus: `<Install Dir>\vsaWs\TestClient\KaseyaWStestClient.exe`
2. Geben Sie den **Benutzernamen** und das **Passwort** eines Benutzers ein, der autorisiert ist, eine Verbindung zum Kaseya Server herzustellen.
3. Wählen Sie die gewünschte Option für den **Hash-Algorithmus** aus. Details finden Sie unter **Authenticate** *(siehe 547)*.

   > **Hinweis:** Das sind derselbe Benutzername und dasselbe Passwort, das ein Administrator für die Anmeldung beim Kaseya Server verwendet.

4. Klicken Sie auf die Schaltfläche **Anmelden**, um einen Wert im Feld **Sitzungs-ID** anzuzeigen.
5. Klicken Sie auf **Durchsuchen**, um eine XML-Testdatei auszuwählen. Dadurch wird der Text der XML-Datei in das Textfeld **SendXML** eingetragen.

Hinweis: Sie brauchen keinen Wert zwischen die <SessionID>-Element-Tags der XML-Nachricht einzugeben. Der **Beispiel-Client** fügt automatisch die angezeigte Sitzungs-ID in jede XML-Nachricht ein, sobald Sie auf die Schaltfläche **Senden** klicken.

6. Klicken Sie auf **Senden**, um die XML-Nachricht an die Ziel-URL zu senden. Im Textfeld **ResponseXML** wird eine XML-Antwortnachricht angezeigt.

API-Beispielseite für ASP

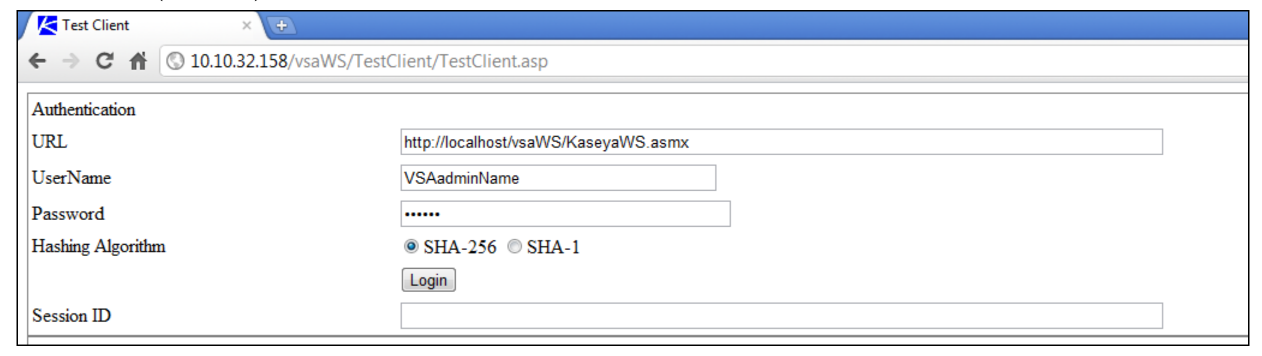
Im Lieferumfang des VSA-API-Webdiensts befindet sich auch eine Testclient-ASP-Seite, die Ihnen hilft, sich mit den verschiedenen API-Vorgängen vertraut zu machen. Sie können daraus ersehen, wie der ASP-Client konstruiert wurde, und auch beliebige Teile dieses Codes in Ihre eigene Anwendung integrieren. Die Benutzer können die tatsächliche Seite unter "/vsaWS/KaseyaWS.asmx" auf einem beliebigen Kaseya Server aufrufen, eine Webmethode auswählen und die exakte XML-SOAP-Anfragestruktur aus der WSDL kopieren und einfügen.

Die Authentifizierung findet in einem eigenen Rahmen am oberen Rand der Seite statt. Die Sitzungs-ID einer erfolgreichen Authentifizierung wird angezeigt und kann kopiert und in nachfolgende XML-Anforderungen eingefügt werden.

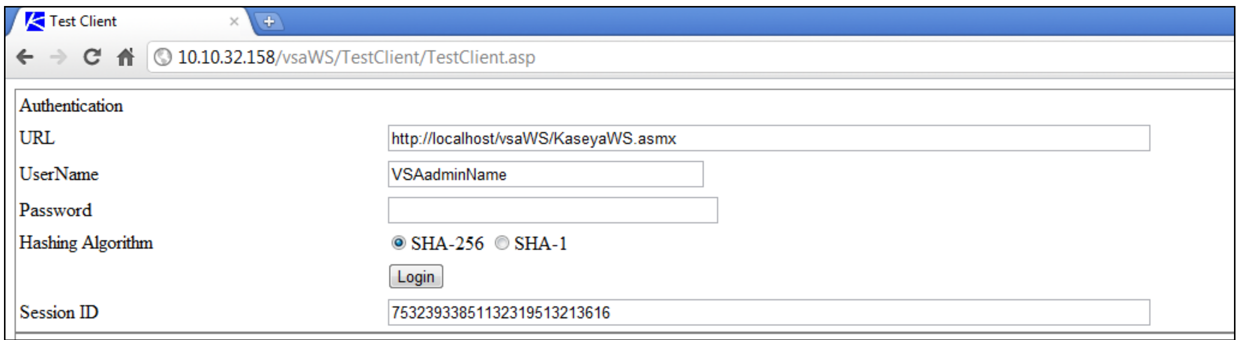
> **Hinweis:** Diese Seite schließt die angezeigte Sitzungs-ID nicht automatisch in nachfolgende Anfrageanweisungen ein, wie dies bei der **API-Beispielanwendung für C#** *(siehe 534)* der Fall ist.

Beispiel 1: Authentifizierung

1. Greifen Sie über `http://<your-KServer>/vsaWS/TestClient/TestClient.asp` auf den ASP-Testclient des VSA-API-Webdiensts zu.
2. Geben Sie einen gültigen Benutzernamen und das Passwort eines VSA-Administrators ein und klicken Sie auf "Anmelden".
3. Wählen Sie die gewünschte Option für den **Hash-Algorithmus** aus. Details finden Sie unter **Authenticate** *(siehe 547)*.

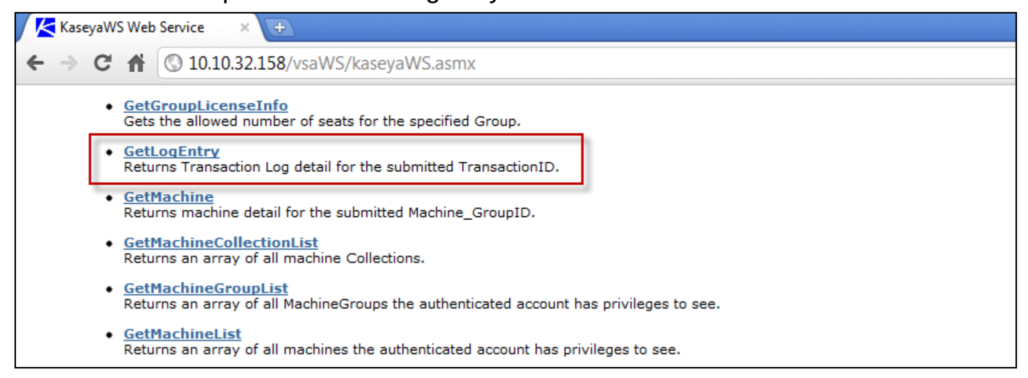


In das Textfeld der Sitzungs-ID wird die bei Ihrer Anmeldung generierte Sitzungs-ID eingetragen. Sie müssen diese Sitzungs-ID kopieren und in nachfolgende XML-Anforderungen einfügen.

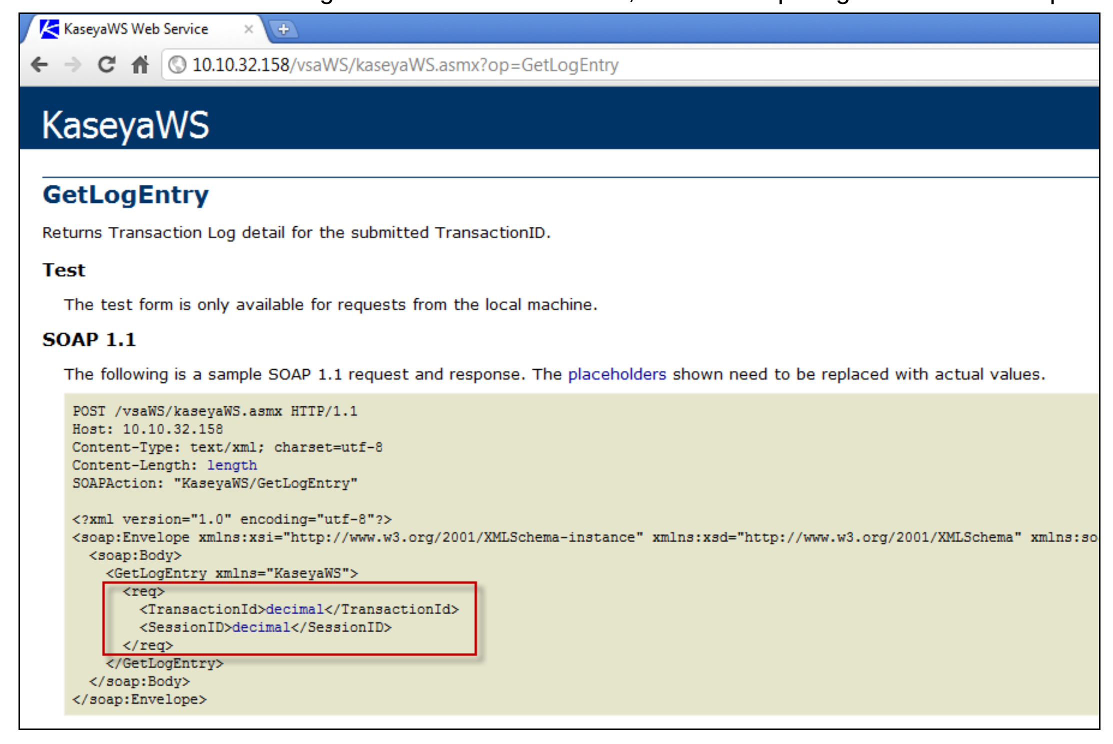


Beispiel 2 - Abrufen-Anforderung erstellen

1. Verwenden Sie in einem zweiten Browser-Fenster die Seite /vsaWS/KaseyaWS.asmx, um eine Methode wie beispielsweise GetLogEntry auszuwählen.

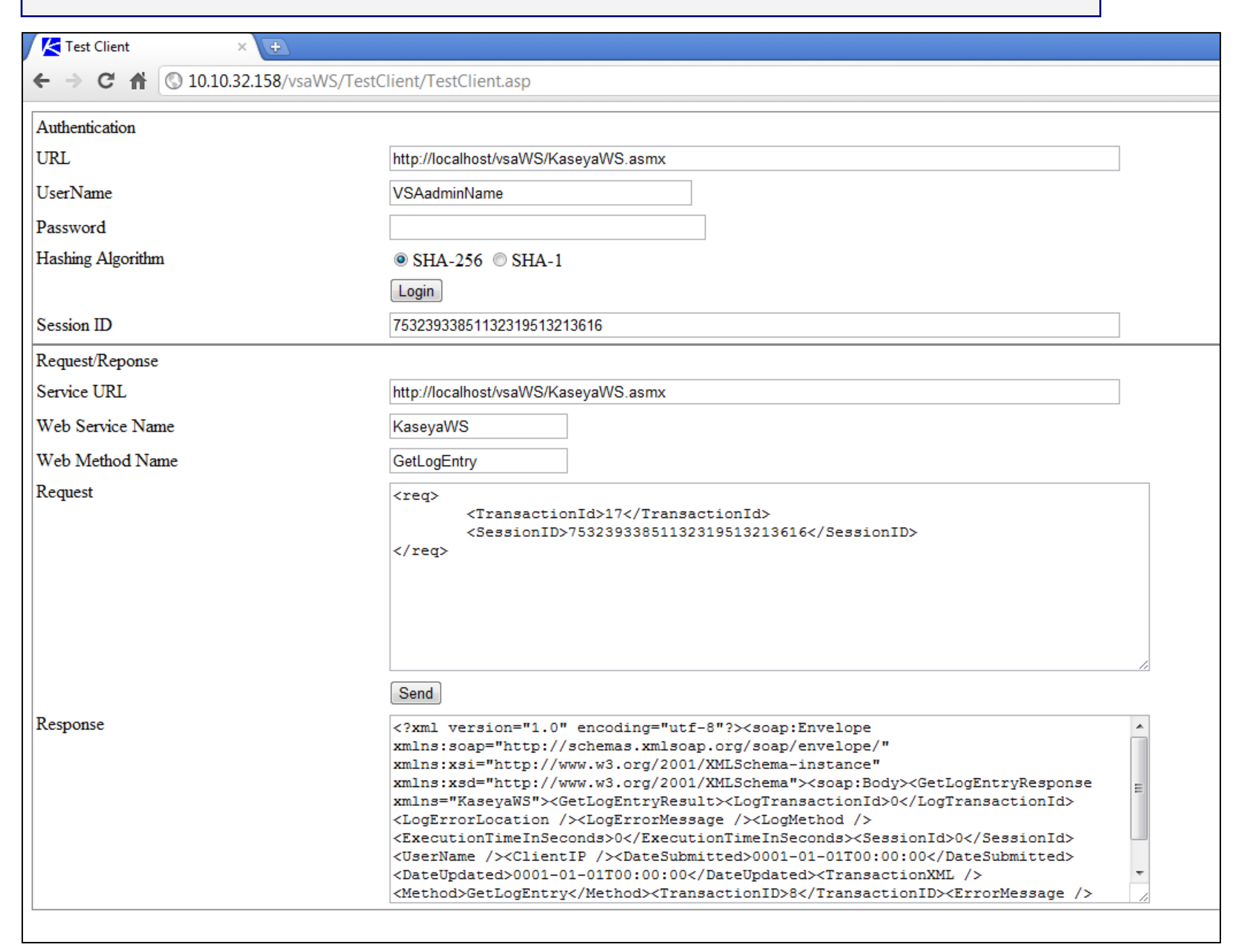


2. Jede Methode zeigt die XML SOAP-Struktur für die Anforderung dieser Methode an. Kopieren Sie nur den Teil der Anfragestruktur dieser Methode, der mit <req> beginnt und mit </req> endet.



3. Fügen Sie die Anforderungsstruktur in den Bereich 'Anforderung' der Seite 'TestClient.asp' ein. Geben Sie den Namen der Methode in das Feld 'Name' der Webmethode ein. Ersetzen Sie den Platzhalter 'Dezimalwert' durch die Sitzungs-ID, die Sie während der Authentifizierung erhalten haben. Ersetzen Sie nach Bedarf andere Platzhalterinhalte durch gültige Daten. Klicken Sie anschließend auf 'Senden'.

> **Hinweis:** Das Element <BrowserIP></BrowserIP> kann in allen Methoden ignoriert werden. Weitere Informationen finden Sie unter **Beschränkung von Anfragen nach IP-Adresse und Benutzer** *(siehe 543)*.



Die Ergebnisse werden im Antwort-Bereich angezeigt.

VSA-API-Webdienst – Sicherheit

Allgemein

Standardmäßig kann auf den VSA-API-Webdienst mit gültigen VSA-Anmeldedaten weltweit von jeder IP-Adresse aus zugegriffen werden. In dieser Standardkonfiguration gelten gültige Kombinationen von Benutzername und Passwort als Authentifizierung von jedem beliebigen Rechner aus.

In jeder Konfiguration muss das Passwort vor dem Senden mit der Datei `hash.dll` verschlüsselt werden, die vom VSA bereitgestellt wird. Implementierungsanweisungen für die Datei `hash.dll` sind im Beispiel-Quellcode enthalten.

Sobald eine erfolgreiche **Authentifizierung**sanforderung eine Sitzungs-ID ausgibt, muss diese Sitzungs-ID bei jedem Dienstaufruf eingesendet werden. Sie ist zudem nur dann gültig, wenn sie von der ID-Adresse empfangen wird, an die sie ausgegeben wurde. Die ausgegebene Sitzungs-ID läuft nach einer bestimmten Periode der Inaktivität ab.

Sie können die Sicherheit erhöhen, indem Sie eine Datei `AccesRules.xml` erstellen und bereitstellen. Anhand dieser Datei kann der VSA-API-Webdienst Zugriffsregeln basierend auf den IP-Adressen definieren, von denen Anfragen empfangen werden. IP-Filterung ist ein Mechanismus, der häufig in Business-to-Business-Systemen eingesetzt wird, um sicherzustellen, dass Anforderungen nur von den Servern des Partners beantwortet werden.

Die Datei `AccessRules.xml` ist in drei Abschnitte unterteilt:

- Standard-Zugriffsregeln
- IP-Bereiche
- Benutzerzuordnung

Hinweis: 127.0.0.1 (localhost) hat immer Zugriff auf jedes Konto, unabhängig von der Konfiguration.

XML-Struktur

```
<AccessRules>
   <DefaultAccessRules>
           <GrantAnyIPToUndefinedUsers/>
           <GrantAllIPRangesToUndefinedUsers/>
           <DenyAccessToUndefinedUsers/>
   </DefaultAccessRules>
   <IPRanges>
           <IPRange RangeID="" FromIPAddress="" ToIPAddress="" RangeDescription=""/>
           <IPRange RangeID="" FromIPAddress="" ToIPAddress="" RangeDescription=""/>
   </IPRanges>
   <UserMapping>
           <User UserName="" RangeID="" GrantAllRanges="" GrantAnyIP="" DenyAccess=""/>
           <User UserName="" RangeID="" GrantAllRanges="" GrantAnyIP="" DenyAccess=""/>
   </UserMapping>
</AccessRules>
```

Standard-Zugriffsregeln

Die Elemente in diesem Abschnitt definieren die Zugriffsregeln für diejenigen Konten, auf die im Abschnitt "Benutzerzuordnung" nicht eigens eingegangen wird.

`<GrantAnyIPToUndefinedUsers/> true/false`

true: Jeder Benutzer nicht in UserMapping erhält Zugriff von jeder IP-Adresse aus.

`<GrantAllIPRangesToUndefinedUsers/> true/false`

true: Jeder Benutzer nicht in UserMapping erhält Zugriff von jeder IP-Adresse in bestimmten IP-Bereichen aus.

`<DenyAccessToUndefinedUsers/> true/false`

true: Jedem Benutzer nicht in UserMapping wird der Zugriff verweigert.

IP-Bereiche

In diesem Abschnitt werden bestimmte Rechner oder Bereiche von Rechnern nach IP-Adresse definiert, über die Benutzerzugriff zugewiesen werden kann.

`RangeID="integer"`

Eine frei vom Benutzer zugewiesene Ganzzahl, über die in UserMapping auf den Bereich verwiesen werden kann.

`FromIPAddress="string"`

Start-IP-Adresse (einschließlich). Die ersten drei Positionen der Vierergruppe müssen der ToIPAddress entsprechen.

`ToIPAddress=" string"`

End-IP-Adresse (einschließlich). Die ersten drei Positionen der Vierergruppe müssen der FromIPAddress entsprechen.

`RangeDescription=" string"`

Beschreibung des IP-Bereichs. Zum Beispiel: "Produktionsserver".

Benutzerzuordnung

`UserName="string"`

Der VSA-Administratorname. Der VSA-API-Webdienst verwendet dieselben Anmeldedaten und dieselbe Passwortverschlüsselung wie der VSA. Falls Sie also Ihr Passwort im VSA ändern, müssen Sie es auch in Ihrer Client-Implementierung des VSA-API-Webdiensts ändern.

`RangeID="integer"`

Hiermit verweisen Sie im Abschnitt "IP-Bereiche" auf einen definierten IP-Bereich. Ein Benutzer kann mehrere UserMapping-Elemente verwenden, um alle IP-Bereiche zu beschreiben, von denen aus er Zugriff besitzt. Diese Funktion wird nicht verwendet, wenn eines der nachstehenden Gewähren-/Ablehnen-Attribute verwendet wird.

`GrantAllRanges="true/false"`

true: Der Benutzer hat Zugriff von jedem im Abschnitt "IP-Bereiche" definierten Bereich.

`GrantAnyIP=" true/false"`

true: Der Benutzer hat Zugriff von jeder IP-Adresse.

`DenyAccess=" true/false"`

true: Der Benutzer hat keinerlei Zugriff.

Beispiel-XML für Zugriffskonfiguration

```
<AccessRules>
   <DefaultAccessRules>
            <GrantAnyIPToUndefinedUsers>false</GrantAnyIPToUndefinedUsers>
            <GrantAllIPRangesToUndefinedUsers>false</GrantAllIPRangesToUndefinedUsers>
            <DenyAccessToUndefinedUsers>true</DenyAccessToUndefinedUsers>
   </DefaultAccessRules>
   <IPRanges>
            <IPRange RangeID="1" FromIPAddress="192.168.214.01" ToIPAddress="192.168.214.10"
RangeDescription="Partner X Production Web Farm"/>
            <IPRange RangeID="2" FromIPAddress="192.168.15.102" ToIPAddress="192.168.15.102"
RangeDescription="Senior Developer Machine"/>
            <IPRange RangeID="3" FromIPAddress="192.168.15.105" ToIPAddress="192.168.15.109"
RangeDescription="Sales Demo Machines"/>
            <IPRange RangeID="4" FromIPAddress="192.168.210.35" ToIPAddress="192.168.210.35"
RangeDescription="Interal QA Machine"/>
   </IPRanges>
   <UserMapping>
            <User UserName="B2BMasterAdmin" RangeID="1" GrantAllRanges="false" GrantAnyIP="false"
DenyAccess="false"/>
            <User UserName="DevTestAccount" RangeID="2" GrantAllRanges="false" GrantAnyIP="false"
DenyAccess="false"/>
            <User UserName="SalesTestAccount" RangeID="3" GrantAllRanges="false" GrantAnyIP="false"
DenyAccess="false"/>
            <User UserName="SalesTestAccount2" RangeID="3" GrantAllRanges="false" GrantAnyIP="false"
```

```
DenyAccess="false"/>
            <User UserName="QAMasterAdmin" RangeID="4" GrantAllRanges="false" GrantAnyIP="false"
DenyAccess="false"/>
            <User UserName="SalesTravellingTestAccount" RangeID="" GrantAllRanges="false"
GrantAnyIP="true" DenyAccess="false"/>
            <User UserName="Bob" RangeID="" GrantAllRanges="true" GrantAnyIP="false" DenyAccess="false"/>
            <User UserName="Sally" RangeID="" GrantAllRanges="false" GrantAnyIP="false"
DenyAccess="true"/>
   </UserMapping>
</AccessRules>
```

Web-Links - Eingehend und ausgehend

Neben API-Vorgängen, auf die weiter unten in diesem Dokument näher eingegangen wird, unterstützt der Kaseya Server auch die folgenden ein- und ausgehenden Links:

Eingehend

Die URL zur Anzeige der Webseite **Ticket** für eine bestimmte Ticket-ID lautet:

`http://...?ticid=<TicketID>`

Zum Beispiel:

`http://demo.kaseya.com?ticid=1234`

Ticket ID: 1041 Associate ticket with: mt-ws002.unnamed
Summary: mt-ws002.unnamed has 10.6% free space left
Submitter Information
Name:
Email:
Phone:
Date Created: 7:33:49 pm 12-Oct-07
Age: 12 days 22 hrs
Date Due: 7:33:49 pm 1-Nov-07
Update
Assignee: < unassigned >
Category: Workstation configuration
Status: Open
Priority: High
SLA Type: None
Dispatch Tech: Yes
Approval: Not required
Hours Worked: 0.00
On site: Yes
Warranty Work: Yes
Billable: Yes
Phone Number:
Contact Email:
Hardware type: Laptop
Blood type: ab-
Number of Siblings: 0
Enter new note
Suppress email notifications
Time/Admin | Note | Hide
7:33:49 pm 12-Oct-07 *Alert* | D: on mt-ws002.unnamed has '2356MB free space (10.6%) on a 115718MB disk drive

Ausgehend

Zum Anpassen des Links **Neues Ticket** auf der Seite **Live Connect** tragen Sie die erforderlichen Angaben entsprechend dem Kommentarabschnitt der folgenden XML in die Datei `externalLink.xml` ein. Legen Sie die `externalLink.xml`-Datei zur Aktivierung des neuen Ticket-Links im `\WebPages\install\`-Verzeichnis Ihres Kaseya Server ab.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<externalLinks>
  <!--
  URL STRING SUBSTITUTIONS: The URL string displayed is associated
  with a particular machine ID. The string is searched for the following
  case sensitive values and substituted for the values below.
```

```
  machineNameVal - the machine name for the active machine is substituted
                   in the URL string.
  groupNameVal - the group name for the active group.
  -->
  <ticketLink displayName="Ext Ticket"
url="http://192.168.212.52/?mname=machineNameVal&amp;gname=groupNameVal"/>
</externalLinks>
```

Kapitel 13

Beschränkung von Anfragen nach IP-Adresse und Benutzer

Bei gewissen Vorgängen, etwa **AddTicRequest** *(siehe 546)*, enthält die Anfrage das Element `<BrowserIP>`.

```
<BrowserIP>string</BrowserIP>
```

Mit diesem Element können Anfragen auf einen bestimmten IP-Adressbereich oder auf ausgewählte Benutzer beschränkt werden. In allen anderen Fällen kann es ignoriert werden.

So aktivieren Sie diese Funktion:

1. Suchen Sie die Datei `AccessRights.xml` im Verzeichnis `<KaseyInstallationDirectory>\vsaWS`.
2. Tragen Sie die gewünschten IP-Adressbereichen und optional Benutzer in die Datei ein.
3. Verschieben Sie die Datei in das Verzeichnis `<KaseyInstallationDirectory>\vsaWS\bin`.
4. Starten Sie IIS neu.

AccessRights.xml

```
<AccessRules>
   <DefaultAccessRules>
           <GrantAnyIPToUndefinedUsers>false</GrantAnyIPToUndefinedUsers>
           <GrantAllIPRangesToUndefinedUsers>false</GrantAllIPRangesToUndefinedUsers>
           <DenyAccessToUndefinedUsers>true</DenyAccessToUndefinedUsers>
   </DefaultAccessRules>
   <IPRanges>
           <IPRange RangeID="1" FromIPAddress="192.168.214.01" ToIPAddress="192.168.214.10" RangeDescription="Partner X
Production Web Farm"/>
           <IPRange RangeID="2" FromIPAddress="192.168.15.102" ToIPAddress="192.168.15.102" RangeDescription="Senior
Developer Machine"/>
           <IPRange RangeID="3" FromIPAddress="192.168.15.105" ToIPAddress="192.168.15.109" RangeDescription="Sales Demo
Machines"/>
           <IPRange RangeID="4" FromIPAddress="192.168.210.35" ToIPAddress="192.168.210.35" RangeDescription="Internal QA
Machine"/>
   </IPRanges>
   <UserMapping>
           <User UserName="B2BMasterAdmin" RangeID="1" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
           <User UserName="DevTestAccount" RangeID="2" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
           <User UserName="SalesTestAccount" RangeID="3" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
           <User UserName="SalesTestAccount2" RangeID="3" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
           <User UserName="QAMasterAdmin" RangeID="4" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="false"/>
           <User UserName="SalesTravellingTestAccount" RangeID="" GrantAllRanges="false" GrantAnyIP="true"
DenyAccess="false"/>
           <User UserName="Bob" RangeID="" GrantAllRanges="true" GrantAnyIP="false" DenyAccess="false"/>
           <User UserName="Sally" RangeID="" GrantAllRanges="false" GrantAnyIP="false" DenyAccess="true"/>
   </UserMapping>
</AccessRules>
```

VSA-API-Webdienst – Vorgänge

Mit dem **VSA-API-Webdienst** können folgende Vorgänge ausgeführt werden.

AddMachGrouptoScope

Fügt einen Rechner nach `GroupName` zum `ScopeName` hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddOrg

Fügt eine Organisation hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

orgOutId	decimal	Die Organisations-ID der neu hinzugefügten Organisation.
orgOutRef	string	Der vollständig qualifizierte Name der Organisation. Verwendet die Punktnotation, falls über- oder untergeordnete Organisationen existieren. Beispiele: ▪ `neworgname` ▪ `parentorgname.neworgname` ▪ `parentorgname.childorgname.neworgname`
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddOrgDepartment

Fügt einer Organisation eine Abteilung hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddOrgDeptStaff

Fügt einen Mitarbeiter zu der Abteilung einer Organisation hinzu.

Ausgewählte Anfragenfelder

- **Status** – Geben Sie 0 ein oder lassen Sie das Feld leer. Wird vom VSA nicht genutzt.

- **Alle Tickets anzeigen** – Wenn wahr, kann der mit diesem Mitarbeiter verknüpfte VSA-Benutzer alle Tickets in seinem Scope sowie die mit diesem spezifischen Mitarbeiterdatensatz verknüpften Tickets anzeigen. Wenn falsch, kann dieser VSA-Benutzer nur die mit diesem spezifischen Mitarbeiterdatensatz verknüpften Tickets anzeigen. Weitere Informationen finden Sie in der Beschreibung der Registerkarte "System > Orgn./Gruppen/Abtlg./Personal > Verwalten > **Personal** *(siehe 426)*".

Antwort

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddOrgToScope

Fügt eine Organisation zu einem Umfang hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddScope

Fügt einen Umfang hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

scopeOutId	decimal	Der Bezeichner des erstellten Scope.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddScopeOrg

Fügt in einem Durchgang eine Organisation und einen Umfang hinzu und verknüpft die Organisation mit dem Umfang.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

orgOutId	decimal	Der Bezeichner der erstellten Organisation.
orgOutRef	string	Der vollständig qualifizierte Name der Organisation. Verwendet die Punktnotation, falls über- oder untergeordnete Organisationen existieren. Beispiele: • `neworgname` • `parentorgname.neworgname` • `parentorgname.childorgname.neworgname`

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddTicRequest

Fügt eine vorläufige Ticketanforderung hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

newId	string	Eindeutiger Identifikator.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddUserToRole

Fügt einer Benutzerrolle einen Benutzer hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddUserToScope

Fügt einem Umfang einen Benutzer hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AdminGroupAccess

Weist einer Benutzerrolle eine Rechnergruppe hinzu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AssignRole

Weist einer Benutzerrolle einen Benutzer zu bzw. entfernt diesen.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AssignScope

Weist einem Umfang einen Benutzer zu bzw. entfernt diesen.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Authenticate

Benötigt für den Start einer VSA-API-Webdienstsitzung. Die zurückgegebene Sitzungs-ID muss mit jeder in der Sitzung aufgerufenen Methode übertragen werden. Die Sitzungs-ID ist nur gültig, wenn sie von dem gleichen Rechner erhalten wird, auf dem auch die Authentifizierung stattfand.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

SessionID	decimal	Die eindeutige Sitzungs-ID, die einer Benutzerverbindung mit der Ziel-URL zugewiesen wird.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Automatische Anmeldung während der Authentifizierung

Wenn Sie sich über die API authentifizieren, werden Sie automatisch beim VSA angemeldet. Falls Sie zum Zeitpunkt der Authentifizierung bereits beim VSA angemeldet sind, werden die beiden Sitzungen synchronisiert. Das Ergebnis ist in beiden Fällen das gleiche – es werden an beiden Ausgangspunkten gültige Sitzungen eingerichtet.

Der VSA sucht in der Abfragezeichenfolge jeder VSA-Seite nach der 26-stelligen Sitzungs-ID der API. Falls die Anwendung den Benutzer also auf eine VSA-Seite umleitet, wird sie geöffnet, ohne dass sich der Benutzer erneut anmelden muss. Die Syntax lautet:

```
URL?apiLogonGuid=12345678901234567890123456
```

Zum Beispiel:

```
http://someServer:123/Systemtab/SomePage?apiLogonGuid=12345678901234567890123456&SomeVar=SomeValue
```

Die API-Aktivität sorgt dafür, dass die VSA-Sitzung aktiv bleibt. Da der VSA jedoch nicht davon ausgeht, dass stets Bedarf für eine API-Sitzung besteht, hält die VSA-Aktivität die API-Sitzung umgekehrt nicht aktiv.

Die API verwendet den gleichen Timeout-Wert wie der VSA, der auf die Seite "System >

Anmelderichtlinie *(siehe 444)* des VSA festgelegt wird. Der Standardwert beträgt 30 Minuten.

Hash-Algorithmus

Ab Version 6.2 implementiert K2 für sichere Authentifizierungen den Hash-Algorithmus SHA-256. Der bisherige Standard war SHA-1. Eine allgemeine Beschreibung dieser Verbesserung finden Sie im Thema **Passwörter externer Anwendungen ändern** *(siehe 413)* der Online-Hilfe zum System.

- Neu erstellte oder zurückgesetzte Passwörter werden mit SHA-256 gehasht.
- Für nicht zurückgesetzte Legacy-Passwörter ist SHA-1 weiterhin erforderlich.
- Der Parameter `HashingAlgorithm` in **Authenticate** wird standardmäßig auf `SHA-1` gesetzt, wenn er nicht eigens angegeben wird.
- Die **API-Beispielanwendung für C#** *(siehe 534)* und die **API-Beispielseite für ASP** *(siehe 536)* bieten eine Option zum Wechseln zwischen SHA1 und SHA-256.
- VSA-Passwörter können nur in der VSA-Anwendung zurückgesetzt werden, nicht über die API.

Warnung: Jegliche Änderung des Passworts einer externen Legacy-Anwendung führt zu einer **Unterbrechung der Integration**, bis entweder die externe Anwendung zur Nutzung des erforderlichen SHA-256-Hash-Algorithmus aktualisiert wurde oder neue SHA-1-Anmeldedaten erstellt und angewendet wurden. Stellen Sie also sicher, dass keine Passwörter externer Anwendungen geändert werden, bevor die Aktualisierung vorgenommen wurde. Siehe **Neue SHA-1-Anmeldedaten für externe Legacy-Anwendungen erstellen** unten.

Best Practices

Für eine nahtlose Migration zwischen früheren Versionen und der aktuellen Version empfiehlt Kaseya, den Clientcode der API-Webdienste so zu programmieren bzw. umzuprogrammieren, damit zunächst die Authentifizierung mit SHA-256 versucht und erst anschließend SHA-1 verwendet wird. Dadurch stellen Sie sicher, dass der Clientcode mit Passwörtern aus früheren Versionen und der aktuellen Version von VSA kompatibel ist.

1. Setzen Sie den Parameter `HashingAlgorithm` in der Anfrage **Authenticate** auf `SHA-256`. Vergewissern Sie sich, dass das Passwort mit SHA-256 gehasht wird. Geben Sie die Anfrage **Authenticate** aus. Prüfen Sie, dass eine gültige Sitzungs-ID zurückgegeben wird.
   - Die Authentifizierung war erfolgreich, wenn der Parameter `SessionID` einen anderen Wert als Null zurückgibt und der Parameter `ErrorMessage` leer ist.
   - Die Authentifizierung war nicht erfolgreich, wenn der Parameter `SessionID` den Wert Null zurückgibt. Führen Sie Schritt 2 aus.
2. Setzen Sie den Parameter `HashingAlgorithm` auf `SHA-1`. Hashen Sie das Passwort erneut, diesmal mit SHA-1. Geben Sie die Anfrage **Authenticate** erneut aus. Prüfen Sie, dass eine gültige Sitzungs-ID zurückgegeben wird.

Neue SHA-1-Anmeldedaten für externe Legacy-Anwendungen erstellen

Wenn Sie in VSA v6.2 oder höher einen kompatiblen Satz aus SHA-1-Benutzernamen und -Passwort für eine externe Legacy-Anwendung anlegen müssen, die noch nicht auf Kompatibilität mit v6.2-Passwörtern aufgerüstet wurde, gehen Sie wie folgt vor: Erstellen Sie entweder einen neuen Master-Benutzer mit zugehörigem Passwort oder setzen Sie das Passwort des bestehenden Master-Benutzers zurück.

Hinweis: Sie müssen über Administratorberechtigungen auf dem Kaseya Server verfügen. Aus Sicherheitsgründen können Sie das folgende Verfahren nicht remote ausführen.

Neues Master-Benutzerkonto erstellen

1. Melden Sie sich auf dem Rechner an, auf dem der Kaseya Server ausgeführt wird.
2. Rufen Sie diese Webseite auf: `http://localhost/localAuth/setAccountV61.asp`.
3. Geben Sie einen neuen Kontonamen in das Feld **Master-Benutzername** ein.

4. Geben Sie ein Passwort in das Feld **Passwort eingeben** ein und bestätigen Sie es, indem Sie es erneut in das Feld **Passwort bestätigen** eingeben.
5. Geben Sie im Feld **E-Mail-Adresse** eine E-Mail-Adresse ein.
6. Klicken Sie auf **Erstellen**.

Die externe Anwendung kann nun aktualisiert werden, um sich über das neue Benutzerkonto und SHA-1-Passwort mit dem VSA zu verbinden.

Passwort eines bestehenden Master-Benutzers zurücksetzen

> **Hinweis:** Das Master-Benutzerkonto kann nicht deaktiviert werden.

1. Melden Sie sich auf dem Rechner an, auf dem der Kaseya Server ausgeführt wird.
2. Rufen Sie diese Webseite auf: `http://localhost/localAuth/setAccountV61.asp`.
3. Geben Sie den Namen eines bestehenden aktiven Master-Benutzerkontos in das Feld **Master-Benutzername** ein.
4. Geben Sie ein Passwort in das Feld **Passwort eingeben** ein und bestätigen Sie es, indem Sie es erneut in das Feld **Passwort bestätigen** eingeben.
5. Überspringen Sie die **E-Mail-Adresse**. Auf dieser Webseite kann die E-Mail-Adresse eines bestehenden Benutzers nicht zurückgesetzt werden.
6. Klicken Sie auf **Erstellen**.

Die externe Anwendung kann nun aktualisiert werden, um sich über das neue SHA-1-Passwort mit dem VSA zu verbinden.

AuthenticateWithAppSessionID

Ruft die API-SessionID einer gültigen AppSession ab. Nur von lokalem Server verfügbar.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

SessionID	decimal	Die eindeutige Sitzungs-ID, die einer Benutzerverbindung mit der Ziel-URL zugewiesen wird.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

> **Hinweis:** Hinweise zum Start einer neuen Sitzung erhalten Sie unter **Authenticate** *(siehe 547)*.

CloseAlarm

Schließt den Alarm für die übertragene MonitorAlarmID. In der VSA-Benutzeroberfläche werden Alarme manuell geschlossen, und zwar auf der Seite "Monitor > **Alarmübersicht** *(siehe 260)*".

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

CreateAdmin

Erstellt einen VSA-Benutzer. Das Passwort muss hash-codiert werden.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

CreateAgentInstallPackage

Erstellt ein Agent-Installationspaket.

Anfrage

```
<?xml version="1.0" encoding="utf-8"?>
<req>
  <GroupName>string</GroupName>
  <DefaultAccount>decimal</DefaultAccount>
  <AgentType>int</AgentType>
  <CommandLineSwitches>string</CommandLineSwitches>
  <PackageName>string</PackageName>
  <PackageDescription>string</PackageDescription>
  <BrowserIP>string</BrowserIP>
  <SessionID>decimal</SessionID>
</req>
```

Wobei:

- `GroupName` – Der Name einer neuen oder bestehenden Rechnergruppe (Schritt 2 im Assistenten zur Paketerstellung)
- `DefaultAccount` – Optional. Agent-GUID eines bestehenden Agents oder einer bestehenden Vorlage, aus dem bzw. der die Einstellung kopiert wird (Schritt 4)
- `AgentType` – -1 = Auto, 0 = Windows, 4 = MAC, 5 = Linux (Schritt 5)
- `CommandLineSwitches` – Selbsterklärend (Schritt 3)
- `PackageNamePackageDescription` – Selbsterklärend (Schritt 7)

Antwort

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

CreateMachineGroup

Erstellt eine Rechnergruppe.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

machGroupGuid	decimal	Die GUID einer erstellten Rechnergruppe
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht

ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

CreateRole

Erstellt eine Benutzerrolle.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteAdmin

Löscht den angegebenen Benutzer.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteAgent

Löscht den Agent auf dem Zielrechner und das entsprechende Rechner-ID-Konto im VSA.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteAgentInstallPackage

Löscht ein Agent-Installationspaket.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteMachineGroup

Löscht die angegebene Rechnergruppe.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteOrg

Löscht die angegebene Organisation.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteRole

Löscht die angegebene Benutzerrolle.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteScope

Löscht den angegebenen Umfang.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DisableAdmin

Deaktiviert den angegebenen Benutzer.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Echo

Testmethode für Verbindungstest und Benchmarking. Erfordert keine Authentifizierung. Gibt die übertragene Zeichenfolge zurück.

Ein einzelner Datensatz des folgenden Felds wird zurückgegeben.

EchoResult	string	Dieser Wert sollte der in die Anforderung eingeschlossenen Eingabe entsprechen.

EchoMt

Testmethode für Verbindungstest und Benchmarking in die mittlere Stufe. Erfordert Authentifizierung. Gibt die übertragene Zeichenfolge zurück. Gibt die übertragene Nutzdaten-Zeichenfolge zurück (Echo).

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Payload	string	Die mit der Anforderung übertragene Zeichenfolge.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

EnableAdmin

Aktiviert den angegebenen Benutzer.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetAlarm

Gibt die Alarmdetails für die übertragene MonitorAlarmID zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Machine_GroupID	string	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
MachineName	string	Der für jeden Agent verwendete Rechnername
GroupName	string	Der für jeden Agent verwendete Gruppenname
MonitorAlarmID	int	Eindeutige Kontrollalarmnummer
MonitorType	int	0 - Zähler 1 - Dienst 2 - Prozess 3 - SNMP 4 - Alarm - Alarme werden weiter nach ihren **Alarmtypen** *(siehe 622)*

		unterteilt. 5 - Systemprüfung 6 - EPS 7 - Protokollkontrolle
AlarmType	string	0 – Alarm 1 – Trending
Message	string	Aus Alarm erstellte Nachricht, Textkörper einer E-Mail-Nachricht
AlarmSubject	string	Betreff des Alarms bzw. der E-Mail-Nachricht
AlarmEmail	string	E-Mail-Adresse(n), an die der Alarm gesendet wird
EventTime	string	Datum und Uhrzeit des Alarms
TicketID	int	Die aus dem erstellte Ticket-ID
AdminName	string	Benutzer, der dem Rechner den Kontrollzähler zugewiesen hat
MonitorName	string	Name des SNMP-Abrufobjekts
LogType		1 – Anwendungsprotokoll 2 – Sicherheitsprotokoll 3 – Systemprotokoll
EventType	int	1 – Fehler 2 – Warnung 4 – Zur Information 8 – Erfolgs-Audit 16 – Fehler-Audit
LogValue	decimal	Wert, der den Alarm auslöst. Falls der Rückgabewert des SNMP-Abrufobjekt-Befehls eine Zeichenfolge ist, ist der Wert diese Nachricht
SNMPName	string	Der vom SNMP-Gerät beim Scan zurückgegebene Wert
SNMPCustomName	string	Benutzerspezifischer Name des SNMP-Geräts
SystemCheckParam1	string	Erster bei der Systemprüfung verwendeter Parameter
SystemCheckParam2	string	(Optional) Zweiter bei der Systemprüfung verwendeter Parameter
MonitorAlarmStateId	int	1 – Geöffnet, 2 – Geschlossen
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetAlarmList

Gibt standardmäßig eine Reihe neuer Alarme zurück, die seit der letzten Anforderung hinzugefügt wurden. Gibt alle Alarme zurück, wenn ReturnAllRecords auf 'Wahr' gesetzt ist.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

Machine_GroupID	string	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID
agentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
MonitorAlarmID	int	Eindeutige Kontrollalarmnummer

AlertType	int	Meldungen sind einer der verschiedenen **Monitortypen** *(siehe 623)* auf. 1 – Adminkonto deaktiviert 2 – Meldung 'Dateiänderung abrufen' 3 – Neuer Agent hat das erste Mal eingecheckt 4 – Anwendung installiert oder gelöscht 5 – Agent-Verfahrensfehler festgestellt 6 – Fehler in NT-Ereignisprotokoll festgestellt 7 – Kaseya Server beendet 8 – Schutzverletzung festgestellt 9 – PCI-Konfiguration geändert 10 – Festplattenlaufwerkskonfiguration geändert 11 – RAM-Größe geändert 12 – Test-E-Mail von serverInfo.asp gesendet 13 – Geplanter Bericht abgeschlossen 14 – LAN-Watch-Meldungstyp 15 – Agent offline 16 – Festplattenspeicher niedrig 17 – Remote Control deaktiviert 18 – Agent online 19 – Neues Patch gefunden 20 – Patch-Pfad fehlt 21 – Patch-Installation fehlgeschlagen 23 – Backup-Meldung
AlarmSubject	string	Betreff des Alarms bzw. der E-Mail-Nachricht
EventTime	dateTime	Datum und Uhrzeit des Alarms
MonitorAlarmStateId	int	1 – Geöffnet, 2 – Geschlossen

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetGroupLicenseInfo

Ruft die zulässige Anzahl von Lizenzen für die angegebene Gruppe ab.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

MaxAgents	int	Die maximale Anzahl der Agents, die für diese Rechnergruppe installiert werden kann.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetLogEntry

Gibt die Transaktionsprotokolldetails für die übertragene Transaktions-ID zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

LogTransactionId	decimal	Die Transaktions-ID des Protokolls.

LogErrorLocation	string	Die Fehlerposition des Protokolls.
LogErrorMessage	string	Die Fehlermeldung des Protokolls.
LogMethod	string	Der Protokollvorgang, der eine Antwort anforderte.
ExecutionTimeInSeconds	decimal	Die zum Beantworten der Anforderung benötigte Protokollzeit.
SessionId	decimal	Die Sitzungs-ID des Protokolls.
UserName	string	Der Benutzername des Protokolls.
ClientIP	string	Die Client-IP-Adresse des Protokolls.
DateSubmitted	dateTime	Das Protokolldatum und die -uhrzeit, zu der die Anforderung übertragen wurde.
DateUpdated	dateTime	Das Protokolldatum und die -uhrzeit, zu der die Antwort zurückgegeben wurde.
TransactionXML	string	Die zum Übertragen der Anforderung verwendete XML-Nachricht.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetMachine

Gibt die Rechnerdetails der übertragenen Machine_GroupID zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Machine_GroupID	string	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
machName	string	Der vollständige Rechnername. Der Rechnername besteht aus allen Zeichen links vom Dezimalkomma.
groupName	string	Der vollständige Gruppenname für dieses Konto. Der Gruppenname besteht aus allen Zeichen rechts vom Dezimalkomma.
Manufacturer	string	Herstellerzeichenfolge (Typ 1)
ProductName	string	Produktnamenzeichenfolge (Typ 1)
MachineVersion	string	Versionszeichenfolge (Typ 1)
SysSerialNumber	string	Seriennummernzeichenfolge (Typ 1)
ChassisSerialNumber	string	Seriennummer des Gehäuses (Typ 3)
ChassisAssetTag	string	Bestandsetikettnummer des Gehäuses (Typ 3)
ChassisType	string	Gehäusetyp (Typ 3)
BusSpeed	string	Geschwindigkeit des externen Bus (in MHz) (Typ 4)
MaxMemorySize	string	Maximale Speichermodulgröße (in MB) (Typ 16 - Maximale Kapazität oder, falls Typ 16 nicht verfügbar ist, Maximale Speichermodulgröße Typ 5)
MaxMemorySlots	string	Anzahl der verknüpften Speicherslots (Anzahl der Speichergeräte in Typ 16 oder, falls Typ 16 nicht verfügbar ist, Anzahl der verknüpften Speicherslots in Typ 5)
ChassisManufacturer	string	Gehäusehersteller (Typ 3)
ChassisVersion	string	Gehäuseversion (Typ 3)

MotherboardManufacturer	string	Hersteller der Hauptplatine (Typ 2)
MotherboardProductCode	string	Produktcode der Hauptplatine (Typ 2)
MotherboardVersion	string	Version der Hauptplatine (Typ 2)
MotherboardSerialNumber	string	Seriennummer der Hauptplatine (Typ 2)
ComputerName	string	Name des Computers
IpAddress	string	IP-Adresse des Computers in a.b.c.d-Notation
SubnetMask	string	Subnetzmaske in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DefaultGateway	string	Standard-Gateway-IP-Adresse in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DnsServer1	string	IP-Adresse von DNS-Server #1 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DnsServer2	string	IP-Adresse von DNS-Server #2 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DnsServer3	string	IP-Adresse von DNS-Server #3 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DnsServer4	string	IP-Adresse von DNS-Server #4 in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
DhcpEnabled	int	0 -> Daten nicht verfügbar, 1 -> DHCP auf Clientcomputer aktiviert, 2 -> Deaktiviert
DhcpServer	string	IP-Adresse des DHCP-Servers in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
WinsEnabled	string	0 -> Daten nicht verfügbar, 1 -> WINS-Auflösung auf dem Clientcomputer aktiviert, 2 -> Deaktiviert
PrimaryWinsServer	string	IP-Adresse des primären WINS-Servers in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
SecondaryWinsServer	int	IP-Adresse des sekundären WINS-Servers in a.b.c.d-Notation. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
ConnectionGatewayIp	int	IP-Adresse in a.b.c.d-Notation, die vom Kaseya Server als Quelladresse des Agent ermittelt wurde. Diese IP ist das Netzwerk-Gateway des Agents. Sie unterscheidet sich von der IP-Adresse, falls sich der Computer beispielsweise hinter NAT befindet. Zeichenfolge ist leer, falls keine Daten verfügbar sind.
OsType	string	Zeichenfolge enthält den Typ des Betriebssystems, wie z. B. NT4, 2000, NT3.51 oder WIN32s. Wird aus Teilen der MajorVersion, MinorVersion und PlatformId abgeleitet.
OsInfo	string	Zeichenfolge enthält zusätzliche Informationen zum Betriebssystem, wie z. B. Build 1381 Service Pack 3. Wird aus Teilen der BuildNumber und CsdVersion abgeleitet.
MajorVersion	decimal	Hauptversionsnummer aus einen GetVersionEx() Windows-Funktionsaufruf abgeleitet.
MinorVersion	string	Nebenversionsnummer aus einen GetVersionEx() Windows-Funktionsaufruf abgeleitet. Falls die PlatformId Win32 für Windows lautet, so weist die MinorVersion 0 auf Windows 95 hin. Lautet die PlatformId Win32 für Windows, weist eine MinorVersion > 0 auf Windows 98 hin.
MacAddr	string	Zeichenfolge, die die physikalische Adresse, d. h. die Media Access Control-Adresse, der Verbindung angibt. Eine MAC-Adresse ist folgendermaßen aufgebaut: 00-03- 47-12-65-77

LoginName	string	Benutzername des gegenwärtig angemeldeten Benutzers. Dieser Wert wird bei jedem Schnell-Check-in aktualisiert. Die Fehlerprotokolldatei des Agents wird bei jeder Änderung aktualisiert.
firstCheckin	dateTime	Zeitstempel der erstmaligen Anmeldung dieses Agents beim System
lastCheckin	dateTime	Zeitstempel der letzten Anmeldung dieses Agents beim System
currentUser	string	Anmeldename des gegenwärtig angemeldeten Benutzers. Leer, falls gegenwärtig niemand angemeldet ist
lastLoginName	string	Anmeldename des letzten Benutzers, der sich bei diesem System angemeldet hat
lastReboot	dateTime	Zeitstempel des letzten Neustarts dieses Systems
agentVersion	int	Versionsnummer des auf diesem System installierten Agents
contactName	string	Der diesem Agent zugewiesene Benutzerkontaktname
contactEmail	string	Die diesem Agent zugewiesene Benutzer-Telefonnummer
contactPhone	string	Die diesem Agent zugewiesene Benutzer-Telefonnummer
contactNotes	string	Mit den Kontaktinformationen für diesen Agent verknüpfte Anmerkungen
enableTickets	int	0, falls dieser Benutzer keinen Zugriff auf Ticketing über die Benutzeroberfläche besitzt
enableRemoteControl	int	0, falls dieser Benutzer keinen Zugriff auf Fernsteuerung über die Benutzeroberfläche besitzt
enableChat	int	0, falls dieser Benutzer keinen Zugriff auf Chat über die Benutzeroberfläche besitzt
credentialName	string	Der Benutzername der für diesen Agent eingerichteten Anmeldedaten (falls zutreffend)
primaryKServer	string	Adresse:Port, zu dem der Agent eine Verbindung für seine primäre Kaseya Server-Verbindung herstellt
secondaryKServer	string	Adresse:Port, zu dem der Agent eine Verbindung für seine sekundäre Kaseya Server-Verbindung herstellt
quickCheckinSecs	int	Die Zeit, die gewartet wird (in Sekunden), bevor der Schnell-Check-in eines anderen Agents stattfindet
agentTempDir	string	Das vom Agent auf diesem System verwendete Arbeitsverzeichnis

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

CpuDesc	string	Beschreibung der CPU (z. B. Pentium III Model 8)
CpuSpeed	int	CPU-Geschwindigkeit in MHz (z. B. 601)
CpuCount	int	Anzahl der Prozessoren (z. B. 1)
TotalRam	int	Betrag des RAM in MByte (z. B. 250)

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

DriveLetter	string	Laufwerksbuchstabe der logischen Festplatte (z. B. C)
TotalSpace	int	Gesamtfestplattenkapazität in MByte (z. B. 28609 für 28.609 GB) Kann Null sein, falls nicht verfügbar.
UsedSpace	int	Belegter Festplattenspeicher in MByte (z. B. 21406 für 21.406 GB). Kann Null sein, falls nicht verfügbar.
FreeSpace	int	Freier Festplattenspeicher in MByte (z. B. 21406 für 21.406 GB). Kann Null sein, falls nicht verfügbar.
DriveType	string	Fixed = Festplatte Removable = Diskette oder andere Wechselmedien CDROM Network = zugeordnetes Netzwerklaufwerk
VolumeName	string	Dem Datenträger zugewiesener Name

FormatType	string	NTFS, FAT32, CDFS usw.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetMachineCollectionList

Gibt eine Aufstellung aller Rechnersammlungen zurück. Zurückgegebene Element können als Argumente in der GetMachineList verwendet werden, um die Ausgabe zu filtern.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

collectionName	string	Der Name der Sammlung.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetMachineGroupList

Gibt eine Aufstellung aller Rechnergruppen zurück, die ein authentifiziertes Konto befugt ist, anzuzeigen. Zurückgegebene Element können als Argumente in der GetMachineList verwendet werden, um die Ausgabe zu filtern.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

groupName	string	Die ID der Rechnergruppe.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetMachineList

Gibt eine Aufstellung aller Rechner zurück, die ein authentifizierter Benutzer befugt ist, anzuzeigen. Unterstützt die optionale Filterung der Rückgabe nach übertragener MachineGroup oder MachineCollection. Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

MachineGroupID	string	Eine gegenwärtig bestehende Rechnergruppe. Wenn diese Angabe leer ist, werden alle Rechner zurückgegeben.
IpAddress	string	Die IP-Adresse des Agent-Rechners
MacAddr	string	Die MAC-Adresse des Agent-Rechners

groupName	string	Der für jeden Agent verwendete Gruppenname
firstCheckin	datetime	Der Zeitpunkt, zu dem sich ein Agent erstmals beim VSA angemeldet hat
agentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetMachineUptime

Gibt eine Aufstellung der Laufzeitstatistiken eines Rechners für die übertragene `AgentGuid` oder `MachineGroup` oder alle Rechner zurück, wenn `ReturnAllRecords` auf "Wahr" gesetzt ist. Mit `rptDate` wird das Aufzeichnungsstartdatum der Berechnung auf das aktuelle Datum gesetzt.

Alle Ausgaben werden einer Sicherheitsfilterung unterworfen, auch das `agentGuid`-Singleton und die `MachineGroup`-Untergruppe. Wenn Sie daher eine `agentGuid` oder `MachineGroup` übertragen, für die Sie keine Anzeigeberechtigung besitzen, wird nichts zurückgegeben.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

agentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
machineName	string	Der vollständige Rechnername. Der Rechnername besteht aus allen Zeichen links vom Dezimalkomma.
totalOnline	int	Die Gesamtzeit in Sekunden, die das System während des gesamten Messungszeitraums online war.
measureTime	int	Die Gesamtzeit in Sekunden, während derer das System gemessen wurde (letzte - älteste - Alarm-Auszeiten).
latestStatDate	dateTime	Der letzte Zeitpunkt, zu dem das System gemessen wurde. Dies ist für gewöhnlich der letzte Agent-Protokolleintrag für ein Offline-System.
olderStatDate	dateTime	Der früheste Zeitpunkt, zu dem das System gemessen wurde.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetNotesList

Gibt eine Aufstellung neuer Ticket-Anmerkungen zurück, die seit der letzten Anforderung hinzugefügt wurden. Generiert ein Maximum von 500 Datensätzen in Datumsreihenfolge und zeichnet die aktuellste Anmeldungsausgabe auf. Die Benutzer können diese Methode einfach so lange ausführen, bis keine Datensätze mehr zurückgegeben werden.

- `AddedSince` – Wenn dieses Datum in die Anfrage aufgenommen wird, wird die Systemstandardeinstellung für "Seit letztem Lesevorgang" außer Kraft gesetzt.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

TicketID	int	Die Ticket-ID.
Author	string	Der Autor der Anmerkung.
DateEntered	dateTime	Das Datum, an dem die Anmerkung erstellt oder zuletzt bearbeitet wurde.
NoteText	string	Der Text der Anmerkung.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetOrgLocation

Gibt die Straßenanschrift der Organisation zurück, einschließlich ihres Längen- und Breitengrads.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

orgId	string	Eindeutiger Identifikator.
orgRef	string	Eindeutiger Name.
partitionId	string	Identifikator des Tenants.
orgName	string	Der Name der Organisation.
street	string	Die Straßenanschrift.
city	string	Der Ort.
usState	string	Das Bundesland.
postalCode	string	Die Postleitzahl.
country	string	Das Land.
countryCode	string	Der Landescode.
longitude	string	Der Längengrad der Organisation.
latitude	string	Der Breitengrad der Organisation.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetOrgTypes

Gibt die Rechnerdetails der übertragenen Machine_GroupID zurück.

Es werden mehrere Datensätze der folgenden Felder zurückgegeben.

orgTypeID	decimal	Eindeutiger Identifikator.
orgTypeRef	string	Der eindeutige Name des Organisationstyps.
status	int	1=Aktiv
description	string	Eine Beschreibung des Organisationstyps.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte

TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetOrgs

Gibt die Organisationen zurück, auf die der angemeldete VSA-Benutzer zugreifen kann.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

orgID	string	Eindeutiger Identifikator.
orgName	string	Der Name der Organisation.
orgRef	string	Eindeutiger Name.
CustomerID	string	Eindeutiger Identifikator des Kunden.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetOrgsByScopeID

Gibt die Organisationen zurück, auf die der angegebene Umfang zugreifen kann.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

orgID	string	Eindeutiger Identifikator.
orgName	string	Der Name der Organisation.
orgRef	string	Eindeutiger Name.
CustomerID	string	Eindeutiger Identifikator des Kunden.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetPackageURLs

Ruft eine Liste aller Agent-Bereitstellungspaket-URLs ab, die dem angemeldeten Benutzer zur Verfügung stehen.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

URL	string	Die URL.
PackageName	string	Der Name des Agent-Bereitstellungspakets.
Description	string	Eine Beschreibung des Agent-Bereitstellungspakets.

AgentType	string	Der Agent-Typ, der eincheckt: 0 = Windows 4 = Apple 5 = Linux

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetPartnerUserLocation

Gibt den Standort eines Tenant-spezifischen VSA-Benutzers samt dem Längen- und Breitengrad des VSA-Benutzers zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

adminId	string	Der eindeutige Bezeichner des VSA-Benutzers
adminName	string	Der Name des VSA-Benutzers
partitionId	string	Der Tenant-Identifikator.
longitude	string	Der Längengrad des VSA-Benutzerstandorts
latitude	string	Der Breitengrad des VSA-Benutzerstandorts
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetPublishedViewColumns

Gibt eine Aufstellung aller Spalten für eine veröffentlichte Datenbankansicht zurück.

> **Hinweis:** Die Dokumentation zu den verfügbaren Datenbankansichten finden Sie unter "**Datenbanksichten > Bereitgestellte Ansichten** *(siehe 484)*".

Es werden mehrere Datensätze der folgenden Felder zurückgegeben.

name	string	Der Name der Datenbankansichtsspalte.
dataType	string	Der Datentyp der Datenbankansichtsspalte.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Beispiel

> **Hinweis:** Das folgende Beispiel wurde anhand der Testseite ausgeführt, die in der jeder Installation unter "http://localhost/vsaWS/testClient/testClient.asp" vorhanden ist.

Anfrage

```
<req>
  <viewName>vScriptLog</viewName>
  <SessionID>42131527423841487151422001</SessionID>
</req>
```

Antwort

```
<GetPublishedViewColumnsResponse>
  <GetPublishedViewColumnsResult>
    <PublishedViewColumns>
      <PublishedViewColumn>
        <name>AdminName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>agentGuid</name>
        <dataType>numeric(26,0)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>EventTime</name>
        <dataType>datetime</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>groupName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>Machine_GroupID</name>
        <dataType>varchar(201)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>machName</name>
        <dataType>varchar(100)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>ScriptDesc</name>
        <dataType>varchar(1000)</dataType>
      </PublishedViewColumn>
      <PublishedViewColumn>
        <name>ScriptName</name>
        <dataType>varchar(260)</dataType>
      </PublishedViewColumn>
    </PublishedViewColumns>
    <Method>GetPublishedViewColumns</Method>
    <TransactionID>3</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetPublishedViewColumnsResult>
</GetPublishedViewColumnsResponse>
```

GetPublishedViewRows

Gibt eine Aufstellung aller Zeilen für eine veröffentlichte Datenbankansicht für eine vorgegebene WHERE-Klausel zurück.

> **Hinweis:** Die Dokumentation zu den verfügbaren Datenbankansichten finden Sie unter "Datenbanksichten > **Bereitgestellte Ansichten** *(siehe 484)*".

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

PublishedViewRows	string	Eine Aufstellung der Zeilendaten.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Beispiel

> **Hinweis:** Das folgende Beispiel wurde anhand der Testseite ausgeführt, die in der jeder Installation unter "http://localhost/vsaWS/testClient/testClient.asp" vorhanden ist.

Anfrage

```
<req>
  <viewName>vScriptLog</viewName>
  <columnsList>AdminName,agentGuid,EventTime,Machine_GroupID,ScriptDesc,ScriptName</columnsList>
  <whereClause>EventTime > DATEADD(hour,4,getdate())</whereClause>
  <orderByList>agentGuid,EventTime</orderByList>
  <ReturnAllRows>false</ReturnAllRows>
  <SessionID>42131527423841487151422001</SessionID>
</req>
```

Äquivalent zu SQL

```
select top 5000 AdminName,agentGuid,EventTime,Machine_GroupID,ScriptDesc,ScriptName
from vScriptLog
where EventTime > DATEADD(hour,-4,getdate())
order by agentGuid,EventTime
```

Wählt 6 von 8 verfügbaren Spalten aus `vScriptLog` aus, in denen in den letzten 4 Stunden eine Aktivität verzeichnet wurde, und sortiert die Ergebnisse zunächst nach Rechner und dann nach Datum der Aktivität.

> **Hinweis:** Wenn `<ReturnAllRows>` auf "Falsch" gesetzt ist, werden die Zeilensätze auf 5000 beschränkt, um die Datenbank vor zu großen Ergebnissätzen zu schützen.

Antwort

```
<GetPublishedViewRowsResponse>
  <GetPublishedViewRowsResult>
    <PublishedViewRows>
      <vScriptLog>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:1905:00</EventTime>
          <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
          <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
          <ScriptName>KES Update AVG via Internet</ScriptName>
        </Row>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:20.00305:00</EventTime>
          <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
          <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
          <ScriptName>KES Update</ScriptName>
        </Row>
        <Row>
          <AdminName>*System*</AdminName>
          <agentGuid>517481450374694</agentGuid>
          <EventTime>20100913T09:24:20.00705:00</EventTime>
```

```
            <Machine_GroupID>xpprox86001.agents.hyperv.kserver</Machine_GroupID>
            <ScriptDesc>Script Summary: Success THEN</ScriptDesc>
            <ScriptName>Run Now  KES Update</ScriptName>
          </Row>
        </vScriptLog>
      </PublishedViewRows>
      <Method>GetPublishedViewRows</Method>
      <TransactionID>4</TransactionID>
      <ErrorMessage/>
      <ErrorLocation/>
    </GetPublishedViewRowsResult>
  </GetPublishedViewRowsResponse>
```


GetPublishedViews

Gibt eine Aufstellung aller veröffentlichten Datenbankansichten zurück.

Hinweis: Die Dokumentation zu den verfügbaren Datenbankansichten finden Sie unter "Datenbanksichten > **Bereitgestellte Ansichten** *(siehe 484)*".

Es werden mehrere Datensätze der folgenden Felder zurückgegeben.

viewName	string	Der Name der Datenbankansicht.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Beispiel

Hinweis: Das folgende Beispiel wurde anhand der Testseite ausgeführt, die in der jeder Installation unter "http://localhost/vsaWS/testClient/testClient.asp" vorhanden ist.

Die Nutzungsdetails jeder Ansicht in dieser Liste werden unter **Datenbanksichten** *(siehe 484)* in der Online-Hilfe und dem Benutzerhandbuch veröffentlicht. Möglicherweise gibt es mehr dokumentierte Gesamtansichten als jene in der über die API publizierten Liste.

Anfrage


```
<req>
  <SessionID>42131527423841487151422001</SessionID>
</req>
```


Antwort


```
<GetPublishedViewsResponse>
  <GetPublishedViewsResult>
    <PublishedViews>
      <PublishedView>
        <viewName>vAddRemoveList</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAdminNotesLog</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAgentConfiguration</viewName>
      </PublishedView>
      <PublishedView>
        <viewName>vAgentLabel</viewName>
      </PublishedView>
      <PublishedView>
```

```
    <viewName>vAlertLog</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vBackupLog</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vBaseApplicationInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vBaseCpuInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vBaseDiskInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vBaseDriveManufacturer</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vBasePciInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vBasePrinterInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vCollectionMember</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vConfigLog</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vCurrApplicationInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vCurrCpuInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vCurrDiskInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vCurrDriveManufacturer</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vCurrPciInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vCurrPrinterInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vEventDetail</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vEventInstanceDetail</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vEventInstanceHistoryDetail</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vkadComputers</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vkadUsers</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vLicenseInfo</viewName>
  </PublishedView>
  <PublishedView>
    <viewName>vMachine</viewName>
  </PublishedView>
  <PublishedView>
```

```
      <viewName>vMonitorAlarmAlert</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vMonitorAlarmCounter</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vMonitorAlarmProcess</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vMonitorAlarmService</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vMonitorAlarmSNMP</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vMonitorAlarmSystemCheck</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vNetStatsLog</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vNtEventLogs</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vOnBoardDeviceInfo</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vPatchApprovalStatus</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vPatchPolicy</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vPatchPolicyMember</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vPatchStatus</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vPortInfo</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vScriptLog</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vScriptStatus</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vSystemInfo</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vTicketField</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vTicketNote</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vTicketSummary</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vUptimeHistory</viewName>
    </PublishedView>
    <PublishedView>
      <viewName>vVproAssetDetails</viewName>
    </PublishedView>
  </PublishedViews>
  <Method>GetPublishedViews</Method>
  <TransactionID>2</TransactionID>
  <ErrorMessage/>
```

```
    <ErrorLocation/>
  </GetPublishedViewsResult>
</GetPublishedViewsResponse>
```

GetRoles

Gibt die Rollen zurück, auf die der angemeldete VSA-Benutzer zugreifen kann.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

RoleID	string	Eindeutiger Identifikator.
IsActive	boolean	Die Rolle ist aktiv oder inaktiv.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetScopes

Gibt die Scopes zurück, auf die der angemeldete VSA-Benutzer zugreifen kann

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

ScopeID	string	Eindeutiger Identifikator.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetSessionDetails

Ruft die Sitzungsdetails aus einer übertragenen AppSessionID oder einer gültigen API-SessionID ab. Die Variante AppSessionID ist nur vom lokalen Server verfügbar.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

adminId	int	Bezeichner des VSA-Benutzers
partitionId	decimal	Bezeichner der Partition
machineIdFil	string	Sitzungswert des Rechnerfilters
activeViewId	int	Sitzungswert der Rechneransicht
groupIdFil	string	Sitzungswert des Gruppenfilters
rowPerPage	int	Sitzungswert für Zeilen pro Seite
startRow	int	Startposition im Ergebnissatz
sortField	string	Sortierfeld des aktuellen Datendokuments
sortOrder	int	Sortierreihenfolge des aktuellen Datendokuments
RoleId	int	Rollenbezeichner
AdminRole	string	Name der Rolle
ScopeId	decimal	Scope-Bezeichner

AdminScope	string	Name des Scope
AppSessionExpiration	dateTime	Sitzungsablauf
adminName	string	VSA-Benutzername
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetTicket

Gibt die Ticketdetails für die übertragene MonitorTicketID zurück.

TicketID	int	Eindeutige ID-Nummer des Trouble-Tickets
Machine_GroupID	string	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
machName	string	Der für jeden Agent verwendete Rechnername
groupName	string	Der für jeden Agent verwendete Gruppenname
TicketSummary	string	Ein kurze Beschreibung des Tickets
Assignee	string	Der Admin-Name, dem dieses Ticket zugewiesen ist
CreatedBy	string	Admin-Name (oder Rechner-ID, falls vom Benutzer angegeben) der Person, die das Ticket erstellt hat
CreationDate	string	Zeitstempel der Ticketerstellung
DueDate	string	Fälligkeitsdatum des Tickets
LastModifiedDate	string	Datum, an dem die letzte Anmerkung für dieses Ticket eingegeben wurde
ResolutionDate	string	Zeitstempel der Schließung des Tickets
UserName	string	Der Name des Absenders.
UserEmail	string	Die E-Mail-Adresse des Absenders
UserPhone	string	Die Telefonnummer des Absenders
MonitorAlarmID	int	Der Bezeichner des Kontrollalarms

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

TicketLabel	string	Die Feldbezeichnung
IntegerValue	int	Der Wert eines Ganzzahlfelds
NumberValue	decimal	Der Wert eines numerischen Felds
StringValue	string	Der Wert eines Zeichenfolgenfelds
ListValue	string	Der Wert eines Listenfelds

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetTicketList

Gibt standardmäßig eine Aufstellung neuer Tickets zurück, die seit der letzten Anforderung hinzugefügt wurden. Gibt alle Tickets zurück, wenn ReturnAllRecords auf 'Wahr' gesetzt ist.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

TicketID	int	Eindeutige ID-Nummer des Trouble-Tickets
Machine_GroupID	string	Eine verkettete Darstellung der Rechner-ID und der damit verknüpften Gruppen-ID.
agentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
TicketSummary	string	Ein kurze Beschreibung des Tickets

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetTicketNotes

Gibt eine Aufstellung der Anmerkungen zurück, die zu dem übertragenen Ticket gehören.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

TicketID	int	Die Ticket-ID.
Author	string	Der Autor der Anmerkung.
DateEntered	dateTime	Das Datum, an dem die Anmerkung erstellt oder zuletzt bearbeitet wurde.
NoteText	string	Der Text der Anmerkung.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetTicRequestTicket

Gibt die mit einer Ticketanforderungs-ID verknüpfte Ticket-ID zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

ticketId	string	Der eindeutige Identifikator des Tickets
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetVerboseMachineGroupList

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

groupName	string	Die ID der Rechnergruppe.
machGroupGuid	string	GUID der Rechnergruppe.
parentGroupGuid	string	GUID der übergeordneten Rechnergruppe, falls vorhanden.
orgFK	string	Externer Schlüssel der Organisation, die die Rechnergruppe enthält.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

LockFunctionAccess

Sperrt den Funktionszugriff der übertragenen Benutzerrolle für die übertragene Basisbenutzerrolle.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

MergeAgent

Führt ein Rechner-ID-Konto, das offline ist, mit einem anderen Rechner-ID-Konto zusammen.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

MoveMachineToAnotherGroup

Verschiebt Rechner in eine andere Gruppe.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Primitive

Darüber hinaus werden die folgenden primitiven Datentypvorgänge durchgeführt. Jeder primitive Vorgang verwendet den gleichen xml-Vertrag wie der entsprechende Mehrspaltenvorgang. Jeder primitive Vorgang gibt einen Zeichenfolgenwert zurück, der weiterer Verarbeitung bedarf.

Primitive	Ergebnis	Datentyp
PrimitiveAddMachGroupToScope	PrimitiveAddMachGroupToScopeResult	Zeichenfolge
PrimitiveAddOrg	PrimitiveAddOrgResult	Zeichenfolge
PrimitiveAddOrgDepartment	PrimitiveAddOrgDepartment	Zeichenfolge
PrimitiveAddOrgDeptStaff	PrimitiveAddOrgDeptStaffResult	Zeichenfolge
PrimitiveAddOrgToScope	PrimitiveAddOrgToScopeResult	Zeichenfolge
PrimitiveAddScope	PrimitiveAddScopeResult	Zeichenfolge
PrimitiveAddScopeOrg	PrimitiveAddScopeOrgResult	Zeichenfolge
PrimitiveAddTicRequest	PrimitiveAddTicRequestResult	Zeichenfolge
PrimitiveAddUserToRole	PrimitiveAddUserToRoleResult	Zeichenfolge
PrimitiveAddUserToScope	PrimitiveAddUserToScopeResult	Zeichenfolge
PrimitiveAssignRole	PrimitiveAssignRoleResult	Zeichenfolge
PrimitiveAssignScope	PrimitiveAssignScopeResult	Zeichenfolge
PrimitiveAuthenticate	PrimitiveAuthenticateResult	Zeichenfolge
PrimitiveCloseAlarm	PrimitiveCloseAlarmResult	Zeichenfolge
PrimitiveCreateMachineGroup	PrimitiveCreateMachineGroupResult	Zeichenfolge
PrimitiveCreateRole	PrimitiveCreateRoleResult	Zeichenfolge
PrimitiveDeleteMachineGroup	PrimitiveDeleteMachineGroupResult	Zeichenfolge
PrimitiveDeleteOrg	PrimitiveDeleteOrgResult	Zeichenfolge
PrimitiveDeleteScope	PrimitiveDeleteScopeResult	Zeichenfolge
PrimitiveEchoMt	PrimitiveEchoMtResult	Zeichenfolge
PrimitiveGetAlarm	PrimitiveGetAlarmResult	Zeichenfolge
PrimitiveGetAlarmList	PrimitiveGetAlarmResult	Zeichenfolge
PrimitiveGetLogEntry	PrimitiveGetLogEntryResult	Zeichenfolge
PrimitiveGetMachine	PrimitiveGetMachineResult	Zeichenfolge
PrimitiveGetMachineCollectionList	PrimitiveGetMachineCollectionListResult	Zeichenfolge
PrimitiveGetMachineGroupList	PrimitiveGetMachineGroupListResult	Zeichenfolge
PrimitiveGetMachineList	PrimitiveGetMachineListResult	Zeichenfolge
PrimitiveGetMachineUptime	PrimitiveGetMachineUptimeResult	Zeichenfolge
PrimitiveGetNotesList	PrimitiveGetNotesListResult	Zeichenfolge
PrimitiveGetOrgLocation	PrimitiveGetOrgLocationResult	Zeichenfolge
PrimitiveGetOrgTypes	PrimitiveGetOrgTypesResult	Zeichenfolge
PrimitiveGetOrgs	PrimitiveGetOrgsResult	Zeichenfolge
PrimitiveGetOrgsByScopeID	PrimitiveGetOrgsByScopeIDResult	Zeichenfolge
PrimitiveGetPartnerUserLocation	PrimitiveGetPartnerUserLocationResult	Zeichenfolge
PrimitiveGetPublishedViewColumns	PrimitiveGetPublishedViewColumnsResult	Zeichenfolge
PrimitiveGetPublishedViewRows	PrimitiveGetPublishedViewRowsResult	Zeichenfolge

PrimitiveGetPublishedViews	PrimitiveGetPublishedViewsResult	Zeichenfolge
PrimitiveGetRoles	PrimitiveGetRolesResult	Zeichenfolge
PrimitiveGetScopes	PrimitiveGetScopesResult	Zeichenfolge
PrimitiveGetTicRequestTicket	PrimitiveGetTicRequestTicketResult	Zeichenfolge
PrimitiveGetTicket	PrimitiveGetTicketResult	Zeichenfolge
PrimitiveGetTicketList	PrimitiveGetTicketListResult	Zeichenfolge
PrimitiveGetTicketNotes	PrimitiveGetTicketNotesResult	Zeichenfolge
PrimitiveGetVerboseMachineGroupList	PrimitiveGetVerboseMachineGroupListResult	Zeichenfolge
PrimitiveMoveMachineToAnotherGroup	PrimitiveMoveMachineToAnotherGroupResult	Zeichenfolge
PrimitiveRemoveUserFromRole	PrimitiveRemoveUserFromRoleResult	Zeichenfolge
PrimitiveRemoveUserFromScope	PrimitiveRemoveUserFromScopeResult	Zeichenfolge
PrimitiveRenameMachine	PrimitiveRenameMachineResult	Zeichenfolge
PrimitiveResetPassword	PrimitiveResetPasswordResult	Zeichenfolge
PrimitiveSetLicenseByOrg	PrimitiveSetLicenseByOrgResult	Zeichenfolge
PrimitiveSetPartnerUserLocation	PrimitiveSetPartnerUserLocationResult	Zeichenfolge
PrimitiveUpdateOrg	PrimitiveUpdateOrgResult	Zeichenfolge
PrimitiveUpdateTicket	PrimitiveUpdateTicketResult	Zeichenfolge
PrimitiveUpdateUser	PrimitiveUpdateUserResult	Zeichenfolge

RemoveUserFromRole

Entfernt einen VSA-Benutzer aus einer Rolle.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

RemoveUserFromScope

Entfernt einen VSA-Benutzer aus einem Scope.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

RenameMachine

Benennt einen Rechner um und weist ihn optional einer anderen Rechnergruppe zu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte

TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

ResetPassword

Setzt das Passwort des angegebenen Benutzers zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

RoleMembership

Weist einen Benutzer einer Benutzerrolle zu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

SendAdminMessage

Eine Nachricht an einen Benutzer senden.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

SetAdminPassword

Setzt das Passwort des angegebenen Benutzers zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

SetGroupLicenseInfo

Legt die maximale Anzahl der Agents fest, die für eine eingegebene Gruppe zulässig sind.
Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

SetLicenseByOrg

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

SetPartnerUserLocation

Legt den aktuellen Längen- und Breitengrad des VSA-Benutzers fest
Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

AdminId	decimal	Der eindeutige Bezeichner des VSA-Benutzers
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

UpdateOrg

Aktualisiert die Informationen einer Organisation.
Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

UpdateTicket

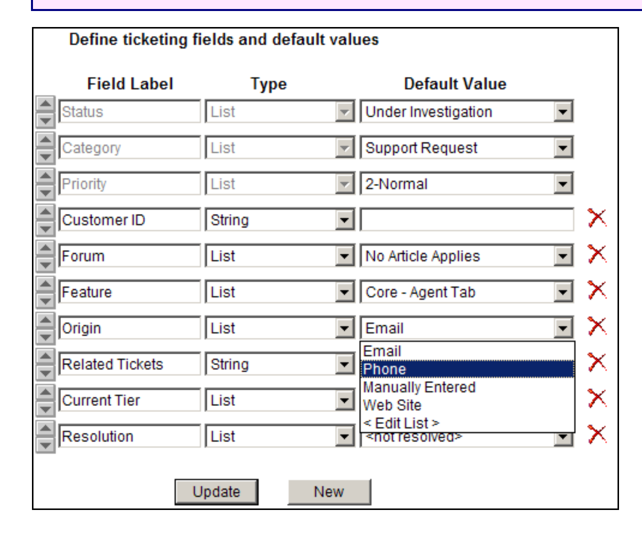
Aktualisiert ein oder mehrere Felder eines Tickets. Nur Felder, die auf der Seite "Ticketing > **Felder bearbeiten** *(siehe 471)*" aufgelistet sind, können aktualisiert werden.

Listenfelder aktualisieren

Im nachstehenden Beispiel ist das Feld `Origin` ein Feld vom Typ `List` mit vier möglichen Werten.

Eine Anfrage übergibt den Namen des Felds (`Origin`) sowie eine Nummer, die die Position des Werts in der Liste angibt (*ab 1 gezählt*). Angenommen, der Wert `Phone` befindet sich an der zweiten Position in der Liste: Der Wert, der zum Ändern des Felds `Origin` in `Phone` übergeben wird, ist gleich `2`.

> **Warnung:** Durch eine Änderung der Reihenfolge der Feld-Dropdown-Liste, indem Sie diese neu ordnen oder in der Mitte der Liste einen neuen Wert eingeben, wird der vom Vorgang **UpdateTicket** ausgewählte Wert geändert. Benutzer müssen sich über diese Integrationsrestriktion im Klaren sein, bevor Änderungen an den Feldwerten unter **Felder bearbeiten** vorgenommen werden.



Ticket schließen

Bei der Aktualisierung eines Tickets kann auch die übertragene MonitorTicketID geschlossen werden, indem das Feld **Status** mit dem Wert `3` aktualisiert wird. Dieser stellt den dritten Wert in der Dropdown-Liste des Felds **Status** dar. Nachstehend wird ein Beispiel angezeigt. Dem nachstehenden Beispiel können weitere Namen/Wert-Elemente für `<TicketField>` hinzugefügt werden, um mehrere Felder zu aktualisieren.

```
<UpdateTicketRequest>
   <TicketID>1</TicketID>
   <TicketFields>
           <TicketField>
                   <Name>Status</Name>
                   <Value>3</Value>
           </TicketField>
   </TicketFields>
   <SessionID>13642146236194247244181221</SessionID>
</UpdateTicketRequest>
```

Andere Typen von Feldern aktualisieren

Die folgenden anderen Typen von Ticketfeldern können aktualisiert werden:

- `String` – Kann Text bis zu einer Länge von 500 Zeichen enthalten. Eignet sich am besten für Angaben, wie die Position eines Problems oder andere Variablen, die nicht in die Übersichtszeile gehören.
- `Integer` – Kann positive oder negative ganzzahlige Werte enthalten.
- `Number (nn.d)` – Zahl mit immer einer Dezimalstelle
- `Number (nn.dd)` – Zahl mit immer zwei Dezimalstellen
- `Number (nn.ddd)` – Zahl mit immer drei Dezimalstellen
- `Number (nn.dddd)` – Zahl mit immer vier Dezimalstellen
- `AddNote` – Fügt dem angegebenen Ticket eine Anmerkung im Nur-Text-Format hinzu.
- `HideNote` – Legt die Eigenschaft "Ausgeblendet" für die hinzugefügte Anmerkung fest.

Bei der Änderung von Feldern durch die Felderaufstellung wird dem angegebenen Ticket eine ausgeblendete Audit-Anmerkung mit Feldname, altem Wert und neuen Wert hinzugefügt. Beispiel: `~API~ [CR] Status has changed from Open to Closed`.

Zurückgegebene Felder

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Ticketanhänge

Der API-Webdienst kann nicht zum Abrufen oder Aktualisieren von Ticket-Dateianhängen verwendet werden. Ticket-Dateianhänge befinden sich gewöhnlich im Verzeichnis `C:\Kaseya\WebPages\ManagedFiles` des Kaseya Server. API-Entwickler müssen Code schreiben, damit Dateianhänge in diesem Verzeichnis abgelegt werden, bevor sie Webdienst-API-Anrufe tätigen.

UpdateUser

Aktualisiert Benutzerdaten.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Hash-Algorithmus

Ab Version 6.2 implementiert K2 für sichere Authentifizierungen den Hash-Algorithmus SHA-256. Der bisherige Standard war SHA-1. Eine allgemeine Beschreibung dieser Verbesserung finden Sie im Thema **Passwörter externer Anwendungen ändern** *(siehe 413)* der Online-Hilfe zum System.

- Neu erstellte oder zurückgesetzte Passwörter werden mit SHA-256 gehasht.
- Für nicht zurückgesetzte Legacy-Passwörter ist SHA-1 weiterhin erforderlich.
- Der Parameter `HashingAlgorithm` in **Authenticate** wird standardmäßig auf `SHA-1` gesetzt, wenn er nicht eigens angegeben wird.
- Die **API-Beispielanwendung für C#** *(siehe 534)* und die **API-Beispielseite für ASP** *(siehe 536)* bieten eine Option zum Wechseln zwischen SHA1 und SHA-256.
- VSA-Passwörter können nur in der VSA-Anwendung zurückgesetzt werden, nicht über die API.

Warnung: Jegliche Änderung des Passworts einer externen Legacy-Anwendung führt zu einer **Unterbrechung der Integration**, bis entweder die externe Anwendung zur Nutzung des erforderlichen SHA-256-Hash-Algorithmus aktualisiert wurde oder neue SHA-1-Anmeldedaten erstellt und angewendet wurden. Stellen Sie also sicher, dass keine Passwörter externer Anwendungen geändert werden, bevor die Aktualisierung vorgenommen wurde. Siehe **Neue SHA-1-Anmeldedaten für externe Legacy-Anwendungen erstellen** unten.

Best Practices

Für eine nahtlose Migration zwischen früheren Versionen und der aktuellen Version empfiehlt Kaseya, den Clientcode der API-Webdienste so zu programmieren bzw. umzuprogrammieren, damit zunächst die Authentifizierung mit SHA-256 versucht und erst anschließend SHA-1 verwendet wird. Dadurch stellen Sie sicher, dass der Clientcode mit Passwörtern aus früheren Versionen und der aktuellen Version von VSA kompatibel ist.

1. Setzen Sie den Parameter `HashingAlgorithm` in der Anfrage **Authenticate** auf `SHA-256`. Vergewissern Sie sich, dass das Passwort mit SHA-256 gehasht wird. Geben Sie die Anfrage **Authenticate** aus. Prüfen Sie, dass eine gültige Sitzungs-ID zurückgegeben wird.
   - Die Authentifizierung war erfolgreich, wenn der Parameter `SessionID` einen anderen Wert als Null zurückgibt und der Parameter `ErrorMessage` leer ist.
   - Die Authentifizierung war nicht erfolgreich, wenn der Parameter `SessionID` den Wert Null zurückgibt. Führen Sie Schritt 2 aus.
2. Setzen Sie den Parameter `HashingAlgorithm` auf `SHA-1`. Hashen Sie das Passwort erneut, diesmal mit SHA-1. Geben Sie die Anfrage **Authenticate** erneut aus. Prüfen Sie, dass eine gültige Sitzungs-ID zurückgegeben wird.

API-Webdienst für Agent-Verfahren

In diesem Abschnitt

API-Webdienst für Agent-Verfahren aktivieren

Eine allgemeine Einführung in die Kaseya-API finden Sie in der Online-Hilfe unter **VSA-API-Webdienst** *(siehe 532)* oder im Benutzerhandbuch.

So aktivieren Sie den API-Webdienst für Agent-Verfahren:

- Öffnen Sie die Seite "System > **Konfigurieren** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#248.htm)*" im VSA.
- Klicken Sie auf das Kontrollkästchen **VSA-API-Webdienst aktivieren**.
- Greifen Sie über `http://<your-KServer>/vsaWS/AgentProcWS.asmx` auf den API-Webdienst für Agent-Verfahren zu.

API-Webdienst für Agent-Verfahren – Vorgänge

Mit dem **API-Webdienst für Agent-Verfahren** können folgende Vorgänge ausgeführt werden.

AddScriptAssignment

Fügt eine scriptAssignment-Zeile zur Ausführung eines RunNow-Skripts hinzu. Der authentifizierte Benutzer muss über Lesezugriff verfügen und für die aktuelle Rolle die Funktion "Planung aktivieren" zugelassen sein.

Ein einzelner Datensatz des folgenden Felds wird zurückgegeben.

ScriptAssignmentId	int	Ein eindeutiger Bezeichner einer Zeile in der Tabelle scriptAssignmentTable, kombiniert aus einer agentGUID und einer scriptID

AddScriptPrompt

Fügt einem Agent-Verfahren verfahrensspezifische Aufforderungsvariablen hinzu. Skripts, die bei der Planung zur Eingabe von Variablen auffordern, speichern die betreffenden Werte in einer Tabelle. Diese Variablen gelten einzig und allein für jede geplante Instanz des Skripts (und nicht für das Skript selbst). Dadurch können mehrere Benutzer dasselbe Skript mit unterschiedlichen Variablen planen. Der authentifizierte Benutzer muss über Lesezugriff auf das Agent-Verfahren verfügen, dem die Aufforderungen hinzugefügt werden.

Ein einzelner Datensatz des folgenden Felds wird zurückgegeben.

AddScriptPromptResult		Es gibt keine Antwort außer einer eventuellen Fehlermeldung.

Echo

Testmethode für Verbindungstest und Benchmarking. Erfordert keine Authentifizierung. Gibt die übertragene Zeichenfolge zurück.

Ein einzelner Datensatz des folgenden Felds wird zurückgegeben.

Echo	string	Dieser Wert sollte der in die Anforderung eingeschlossenen Eingabe entsprechen.

EchoMt

Testmethode für Verbindungstest und Benchmarking in die mittlere Stufe. Erfordert Authentifizierung. Gibt die übertragene Zeichenfolge zurück. Gibt die übertragene Nutzdaten-Zeichenfolge zurück (Echo).

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Payload	string	Die mit der Anforderung übertragene Zeichenfolge.
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetScriptAssignmentId

Ruft die scriptAssignmentId einer Kombination aus scriptId und agentGuid ab.

Ein einzelner Datensatz des folgenden Felds wird zurückgegeben.

ScriptAssignmentId	int	Ein eindeutiger Bezeichner einer Zeile in der Tabelle scriptAssignmentTable, kombiniert aus einer agentGUID und einer scriptID

GetScriptIdFromScriptName

Gibt eine Aufstellung von Skriptobjekten mit grundlegenden Informationen über alle Skripts mit dem Anfragenamen zurück. Es werden nur Skripts mit Lesezugriff des authentifizierten Benutzers zurückgegeben.

Ein einzelner Datensatz der folgenden Felder wird zurückgegeben.

ScriptId	int	Der eindeutige Bezeichner des Skripts
ScriptName	string	Der Name des Skripts
TreePath	string	Die Position des Skripts in der Ordnerstruktur

Monitoring-API-Webdienst

In diesem Abschnitt

Monitoring-API-Webdienst aktivieren

Eine allgemeine Einführung in die Kaseya-API finden Sie in der Online-Hilfe unter **VSA-API-Webdienst**

(siehe 532) oder im Benutzerhandbuch.

So aktivieren Sie den Monitoring-API-Webdienst:

- Öffnen Sie die Seite "System > **Konfigurieren** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#248.htm)*" im VSA.
- Klicken Sie auf das Kontrollkästchen **VSA-API-Webdienst aktivieren**.
- Greifen Sie über `http://<your-KServer>/vsaWS/monitoringWS.asmx` auf den Monitoring-API-Webdienst zu.

Monitoring-API-Webdienst – Vorgänge

Mit dem **Monitoring-API-Webdienst** können folgende Vorgänge ausgeführt werden.

AssignEventAlertToMachine

Weist einem Rechner eine Ereignismeldung zu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

NewId	int	Der eindeutige Bezeichner der Ereignismeldung
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AssignEventLogMachineSettings

Weist einem Rechner Ereignisprotokolleinstellungen zu.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

NewId	int	Der eindeutige Bezeichner der Zuweisung von Ereignisprotokolleinstellungen
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

CreateEventSet

Erstellt einen neuen Ereignissatz. Gibt die ID des neuen Ereignissatzes zurück.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

NewId	int	Der eindeutige Bezeichner des neuen Ereignissatzes
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

CreateEventSetDefinition

Erstellt eine Ereignissatzdefinition.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

NewId	int	Der eindeutige Bezeichner der neuen Ereignissatzdefinition
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteAllEventAlertsFromMachine

Löscht alle einem Rechner zugewiesenen Ereignismeldungen.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteAllEventLogMachineSettings

Löscht allen einem Rechner zugewiesenen Rechnereinstellungen für Windows-Ereignisprotokolle.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteEventAlertFromMachine

Löscht spezifische Ereignismeldungen nach Ereignisprotokolltyp und Kategorie.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteEventLogMachineSettings

Löscht einem Rechner zugewiesene Rechnereinstellungen für Windows-Ereignisprotokolle nach Ereignisprotokolltyp.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteEventSet

Löscht einen Ereignissatz und alle zugehörigen Definitionen.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

DeleteEventSetDefinition

Löscht eine Ereignissatzdefinition nach Ereignissatzdefinitions-ID.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetEventAlertList

Ruft die einem Rechner zugewiesenen Ereignismeldungen ab.

Es werden mehrere Datensätze der folgenden Felder zurückgegeben.

AgentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
AlertEmail	string	E-Mail-Adressen, denen eine Meldung zugestellt wird.
EventLogTypeId	int	Eindeutige ID-Nummer dieses Ereignisprotokolls. Zum Beispiel: Anwendung -> 796450521 DNS-Server -> 1208407329 Sicherheit -> 1664713117 System -> 1380569194 Wenn der Ereignisprotokolltyp von einem Windows-Rechner bezogen wird, wird er in dieser Tabelle mit einer eindeutigen ID erstellt, falls er noch nicht vorhanden ist. Diese ID bleibt in allen Systemen gleich, da bei der Generierung der ID auf den Namen zurückgegriffen wird.
EventLogCategoryValue	int	1 – Fehler 2 – Warnung 4 – Zur Information 8 – Erfolgs-Audit 16 – Fehler-Audit 256 – Kritisch 512 – Ausführlich
EventSetId	int	Der eindeutige Bezeichner des Ereignissatzes
AgentProcedureId	int	Der eindeutige Bezeichner des Agent-Verfahrens, das ausgeführt werden soll, wenn eine Meldung erstellt wird {0} oder null = Kein Skript ausführen
AgentProcedureMachGuid	decimal	Der eindeutige Bezeichner des Rechners, auf dem das Agent-Verfahren ausgeführt wird

CreateTicket	boolean	Wenn wahr, wird bei Erstellung einer Meldung ein Ticket generiert
SendEmail	boolean	Wenn wahr, wird bei Erstellung einer Meldung eine E-Mail versendet
CreateAlarm	boolean	Wenn wahr, wird bei Erstellung einer Meldung ein Alarm generiert
CriteriaType	int	Die Kriterien für die Auslösung einer Meldung 0, null = Einzelereignis 1 = mehrere Ereignisse im Zeitraum 2 = fehlendes Ereignis im Zeitraum
EventCount	int	Anzahl der aufgetretenen Ereignisse, bevor eine Meldung ausgelöst wird
AlarmDurationSecs	int	Anzahl der Sekunden, die abgewartet werden, bevor eine Meldung ausgelöst wird
AlarmRearmSec	int	Anzahl der Sekunden, die nach einem Ereignis abgewartet werden, bevor für dieselben Kriterien eine neue Meldung ausgelöst wird

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetEventLogMachineSettingsList

Gibt die Ereignisprotokolleinstellungen eines bestimmten Rechners zurück.

Es werden mehrere Datensätze der folgenden Felder zurückgegeben.

MachineName	string	Der vollständige Rechnername. Der Rechnername besteht aus allen Zeichen links vom Dezimalkomma.
AgentGuid	decimal	Ein global eindeutiger Bezeichner eines Rechner-ID/Gruppen-ID-Kontos und seines entsprechenden Agents.
EventLogTypeId	int	Eindeutige ID-Nummer dieses Ereignisprotokolls. Zum Beispiel: Anwendung -> 796450521 DNS-Server -> 1208407329 Sicherheit -> 1664713117 System -> 1380569194 Wenn der Ereignisprotokolltyp von einem Windows-Rechner bezogen wird, wird er in dieser Tabelle mit einer eindeutigen ID erstellt, falls er noch nicht vorhanden ist. Diese ID bleibt in allen Systemen gleich, da bei der Generierung der ID auf den Namen zurückgegriffen wird.
EventLogName	string	Der Name des Ereignisprotokolltyps
EventAssignValue	int	Wert zur Bestimmung der Ereignistypen, die aus dem Ereignisprotokoll bezogen werden. Werden als Bitmaps mit der folgenden Wichtigkeit gespeichert: 1 – Fehler 2 – Warnung 4 – Info 8 – Erfolgs-Audit 16 – Fehler-Audit 256 – Kritisch 512 – Ausführlich

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte

TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetEventSetDefinitionList

Gibt eine Ereignissatzdefinition zurück.

Es werden mehrere Datensätze der folgenden Felder zurückgegeben.

EventSetId	int	Der eindeutige Bezeichner des Ereignissatzes
Ignore	int	0, null – Zur Anwendung dieser Filtereinstellungen mit LIKE 1 – Zur Anwendung dieser Filtereinstellungen mit NOT LIKE
Source	string	Filter für das Quelle-Feld des Ereignisprotokolls
Category	string	Filter für das Kategorie-Feld des Ereignisprotokolls
EventId	int	Filter für das Ereignis-ID-Feld des Ereignisprotokolls
UserName	string	Filter für das Benutzername-Feld des Ereignisprotokolls
Description	string	Filter für das Beschreibung-Feld des Ereignisprotokolls
EventSetDefId	int	Der eindeutige Bezeichner der Ereignissatzdefinition

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetEventSetList

Gibt eine Liste von Ereignissätzen zurück.

Es werden mehrere Datensätze der folgenden Felder zurückgegeben.

SetName	string	Der Name eines Ereignissatzes
EventSetId	int	Der eindeutige Bezeichner des Ereignissatzes

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

KSD-API-Webdienst

In diesem Abschnitt

KSD-API-Webdienst aktivieren

Eine allgemeine Einführung in die Kaseya-API finden Sie in der Online-Hilfe unter **VSA-API-Webdienst** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#3433.htm)* oder im Benutzerhandbuch.

So aktivieren Sie den KSD-API-Webdienst:

- Öffnen Sie die Seite "System > **Konfigurieren** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#248.htm)*" im VSA.
- Klicken Sie auf das Kontrollkästchen **VSA-API-Webdienst aktivieren**.
- Greifen Sie über `http://<your-KServer>/vsaWS/vsaServiceDeskWS.asmx` auf den KSD-API-Webdienst zu.

Datentypen des KSD-API-Webdienstes

Es folgt eine Beschreibung der hauptsächlichen Datentypen, die im **KSD-API-Webdienst** verwendet werden. Diese Datentypen werden im XML-Schemadokument in der Datei `XML\Schemas\ServiceDesk\ServiceDeskDefinition.xsd` im Verzeichnis, in dem die Kaseya-Software installiert ist, definiert.

> **Hinweis:** Die Namensbezeichnung `(content)` in den folgenden Beschreibungen bedeutet den Inhalt des Elements.

Beschriftung

- A – AddIncident
- G – GetIncident
- L – ListIncidents
- U – UpdateIncident

RefItem

RefItem beschreibt ein Element, das ein Referenzelement im Service-Desk darstellt. Diese Elemente verfügen über einen internen Datenbank-ID-Wert, einen internen Namen, eine optionale Beschreibung und einen Anzeigewert.

G	ref	string	Der interne Name des Elements. Diesem sind normalerweise der Service-Desk-Name und `||`, beispielsweise `Standard||Open`, vorangestellt.
G	id	string	Der interne Datenbankschlüssel für das Element
G	description	string	Die optionale Beschreibung des Elements
G	(content)	string	Das vom Benutzer lesbare Format des Elements

CustomField

CustomField beschreibt den Wert eines benutzerdefinierten Feldes in einem Vorfall.

AGU	fieldName	string	Der Name des Feldes im Service-Desk
AGU	(content)	string	Der Wert des benutzerdefinierten Feldes

Hinweis

Note beschreibt eine einzelne an ein Ticket angehängte Anmerkung.

G	User	string	Der Name des Benutzers, der die Anmerkung erstellte
G	Timestamp	dateTime	Die Uhrzeit, zu der die Anmerkung erstellt wurde
AG	Text	string	Der Inhalt der Anmerkung. Dieser kann im HTML-Format vorliegen und Verweise auf Anhänge enthalten.
AG	Hidden	boolean	Wahr, wenn die Anmerkung ausgeblendet sein soll
AG	HoursWorked	Decimal	Die Anzahl der Stunden, die an der Aktualisierung des Tickets gearbeitet wurde
AG	SuppressNotify	Boolean	Wahr, wenn Benachrichtigungen für diese Aktualisierung unterdrückt werden sollen

Anhang

Attachment beschreibt einen einzelnen Anhang für das Ticket.

A	Name	string	Eine eindeutige, identifizierende Zeichenfolge für diesen Anhang
A	DisplayName	string	Der Name des Anhangs, wie er dem Benutzer angezeigt wird
A	FileName	string	Der Originalname der Datei oder URL
A	DocumentType	string	Das MIME-Format des Anhangs
A	Content	Base64Binary	Der im binären 64-Basiscode verschlüsselte Inhalt des Anhangs

RelatedIncident

RelatedIncident ist ein weiterer Vorfall, der mit diesem aktuellen Vorfall verbunden wurde.

AGU	IncidentNumber	string	Der eindeutige Identifikator des Vorfalls
G	Summary	string	Die Zusammenfassung des verwandten Vorfalls
G	Status	string	Der vom Benutzer lesbare Status des verwandten Vorfalls
G	Description	string	Das Beschreibungsfeld des Vorfalls

ServiceDeskDefinition

Die folgenden zurückgegebenen **ServiceDeskDefinition**-Elemente beschreiben die Desk-Definition, die zum Bearbeiten des Tickets verwendet wird. Dies stellt jeden der möglichen Werte für jedes Feld im Ticket bereit.

Es wird ein einzelner Datensatz der folgenden Elemente zurückgegeben.

ServiceDeskDefinition	id="decimal"	Ein eindeutiger Identifikator
Name	string	Der Name der Desk-Definition
Description	string	Eine kurze Beschreibung der Desk-Definition
RequireTime	boolean	Wenn wahr, müssen Arbeitsstunden eingegeben werden
DisplayMachineInfo	boolean	Wenn wahr, wird ein Rechnersuchfeld angezeigt
RequireMachineInfo	boolean	Wenn wahr, ist eine Rechnersuchverknüpfung erforderlich
DisplayOrgInfo	boolean	Wenn wahr, wird ein Organisationssuchfeld angezeigt

RequireOrgInfo	boolean	Wenn wahr, ist eine Organisationssuchverknüpfung erforderlich
DisplayCI	boolean	Veraltet
RequireCI	boolean	Veraltet
AllAdmins	boolean	Veraltet
AutoStartClock	boolean	Wenn wahr, wird automatisch eine Uhr gestartet, wenn der Benutzer mit der Bearbeitung des Feldes beginnt
AutoSaveClock	boolean	Wenn wahr, wird beim Speichern des Tickets der Unterschied zwischen der aktuellen Uhrzeit und der Startzeit als Arbeitsstunden eingegeben
AutoInsertNote	boolean	Wenn wahr, werden automatisch Anmerkungen für die am Ticket vorgenommenen Änderungen zum Ticket hinzugefügt
AutoInsertNoteHidden	boolean	Wenn wahr, werden automatisch erstellte Anmerkungen ausgeblendet
NeedStatusNote	boolean	Veraltet
SDPrefix	string	Der zum Anfang der Ticket-ID hinzugefügte Präfixcode
DefaultStatus	decimal	Standardmäßiger Statuswert. Bezieht sich auf eins der Elemente mit dem übereinstimmenden ID-Attribut im Abschnitt "Status".
DefaultStage	decimal	Standardmäßiger Phasenwert. Bezieht sich auf eins der Elemente mit dem übereinstimmenden ID-Attribut im Abschnitt "Phase".
DefaultPriority	decimal	Standardmäßiger Prioritätswert. Bezieht sich auf eins der Elemente mit dem übereinstimmenden ID-Attribut im Abschnitt "Priorität".
DefaultSeverity	decimal	Standardmäßiger Schweregradwert. Bezieht sich auf eins der Elemente mit dem übereinstimmenden ID-Attribut im Abschnitt "Schweregrad".
DefaultResolution	decimal	Standardmäßiger Auflösungswert. Bezieht sich auf eins der Elemente mit dem übereinstimmenden ID-Attribut im Abschnitt "Auflösung".
DefaultCategory	decimal	Standardmäßiger Kategorienwert. Bezieht sich auf eins der Elemente mit dem übereinstimmenden ID-Attribut im Abschnitt "Kategorie".
DefaultSubCategory	decimal	Veraltet
DefaultServiceDesk	boolean	Wenn wahr, ist dies das Standard-Service-Desk, und zwar das erste, das beim Erstellen neuer Tickets ausgewählt wurde
TemplateName	string	Die Vorlagendatei, die anfänglich zum Erstellen des Service-Desks verwendet wurde. Wird ansonsten nicht verwendet.
TemplateType	int	Der Typ des Service-Desks. 1=Ticket, 3=Knowledge Base.
SequenceName	string	Nur zur Verwendung durch die interne Entwicklung
EditingTemplate	string	Der Name des Formulars, das zum Bearbeiten von Tickets für das Service-Desk verwendet wird
ShowNotesPane	boolean	Wenn wahr, wird das Anmerkungsfeld unten in der Tickets-Tabelle angezeigt.
ShowWorkOrders	boolean	Wenn wahr, werden Arbeitsauftrag und Arbeitsauftragsposition im Ticketeditor angezeigt.
ShowSessionTimers	boolean	Wenn wahr, werden Sitzungstimer im Ticketeditor angezeigt.
ShowTasks	boolean	Wenn wahr, werden die Registerkarten "Aufgaben" und aufgabenbezogene Felder angezeigt.
EstimatedHours	double	Die geschätzte Gesamtzahl der Stunden, die zur Lösung des Tickets erforderlich sind
ActualHours	double	Die geschätzte Gesamtzahl der Stunden, die zur Lösung des Tickets eingegeben wurden
EmailReader	string	Das mit dem Service-Desk verknüpfte E-Mail-Leseprogramm
Administrator	string	Der Benutzer, der als "Desk-Administrator" des Service-Desks fungiert. Der Desk-Administrator wird über bestimmte Fehler im Service-Desk

		benachrichtigt.
DefaultPolicy	string	Die dem Desk zugewiesene Standardrichtlinie
Status	RefItem	Gibt eine Liste von untergeordneten Elementen jedes Statuswerts im Service-Desk aus.
Priority	RefItem	Gibt eine Liste von untergeordneten Elementen jedes Prioritätswerts im Service-Desk aus.
Severity	RefItem	Gibt eine Liste von untergeordneten Elementen jedes Schweregradwerts im Service-Desk aus.
Resolution	RefItem	Gibt eine Liste von untergeordneten Elementen jedes Auflösungswerts im Service-Desk aus.
TaskStatus	RefItem	Gibt eine Liste von untergeordneten Elementen jedes Aufgabenstatuswerts im Service-Desk zurück.
Categories	RefItem	Gibt eine Liste von untergeordneten Elementen jedes Kategorienwerts im Service-Desk aus.
Stages		Gibt eine Liste von untergeordneten Elementen jedes Phasenwerts im Service-Desk aus. Jede Phase wird durch ein "Anfang"-, "Mitte"- oder "Ende"-Phasentypattribut identifiziert. Jede Phase verfügt über die folgenden untergeordneten Elemente: • Item – Der Name der Phase • Initialization – Das mit der Phase verknüpfte Phaseneingangsverfahren • Escalation – Das mit der Phase verknüpfte Eskalationsverfahren. Uhrzeit und Einheiten werden als Attribute angegeben. • Goal – Das mit der Phase verknüpfte Ziel. Das mit der Phase verknüpfte Zielverfahren. Uhrzeit und Einheiten werden als Attribute angegeben. • NextStage – Eine der nächsten Phasen, in die diese Phase übergehen kann
Participants	RefItem	Die Liste der Benutzer als Pools, die Administratoren oder Eigentümer des Service-Desks sein können
CurrentContact		Kontaktinformationen über den Benutzer, der während dieser Transaktion angemeldet ist. Wenn der Benutzer mit einem Mitarbeiterdatensatz verknüpft ist, werden die Informationen für `CurrentContact` diesem Datensatz entnommen. Falls der aktuell angemeldete Benutzer ein Rechnerbenutzer mit **Portalzugriff** ist, werden die Informationen für `CurrentContact` der Registerkarte "Startseite > Profil ändern" des **Portalzugriffs** entnommen. • ContactName • PhoneNumber • Organisation • EmailAddress
SubmitterTypes	string	Der Typ der Person, die das Ticket übermittelt: • UNBEKANNT • TEILNEHMER – Ein Teilnehmer ist ein VSA-Benutzer. • BENUTZER – Eine dem VSA unbekannte Person

CustomFields		Gibt keine oder mehrere Feldelemente aus, jedes mit der folgenden Hierarchie: • Caption – Bildschirmtitel • Title – Berichtstitel • Fieldname – Name des Feldes • FieldFormat – Datentyp • DefaultValue – Standardwert, wenn Listendatentyp • Values – Gruppenelement, wenn Listendatentyp Item – Listenelementwert
AccessRights		Gibt eine Hierarchie von untergeordneten Elementen aus: • ViewHiddenNotes – wahr oder falsch • ChangeHiddenNotes – wahr oder falsch • Feldberechtigungen>Feldberechtigung – Sammlungselemente FieldName – Name des Ticketfeldes AccessType – Erforderlich, Bearbeiten, Nur Ansicht, Ausgeblendet
NoteTemplates		Gibt eine Liste von Anmerkungsvorlagen aus, von denen jede Standardtest darstellt, der zu Ticketanmerkungen hinzugefügt werden kann.
ChangeProcedure	string	Das mit dem Service-Desk verknüpfte Ticketänderungsverfahren
GoalProcedure	decimal	Das mit dem Service-Desk verknüpfte Zielverfahren • time – Der Zeitraum für Ziel • unit – Die Zeiteinheiten • (content) – Der Name des Zielverfahrens
ResourceTypes		Die Liste der Ressourcentypen, die einem Ticket zugewiesen werden können
TaskDefinitions		Die Liste der Aufgabenwerte, die einem Aufgabenstatus zugewiesen werden können
AssocPolicies		Die Liste der Richtlinien, die mit einem Ticket verknüpft werden können

IncidentSummary

Die Vorfallübersicht **IncidentSummary** enthält eine einfache Beschreibung eines Tickets.

AGLU	ServiceDeskName	string	Der Name der Desk-Definition
GLU	IncidentNumber	string	Der Ticketidentifikator
AGLU	Summary	string	Der Text der Ticketübersicht
AGLU	Description	string	Der Text der Ticketbeschreibung
AGLU	Status	string	Der Referenzstatus des Tickets
AGLU	Priority	string	Die Referenzpriorität des Tickets
AGLU	Resolution	string	Der Referenzauflösungstyp des Tickets
AGLU	Stage	string	Die Referenzphase des Tickets
AGLU	Severity	string	Der Referenzschweregrad des Tickets
AGLU	Category	string	Die Referenzkategorie des Tickets
AGLU	SubCategory	string	Die Referenzunterkategorie des Tickets
GL	Policy	string	Die Richtlinie des Tickets
GL	CreateDateTime	dateTime	Das Datum/die Uhrzeit der Erstellung des Tickets
GL	LastEditDateTime	dateTime	Das Datum/die Uhrzeit der letzten Bearbeitung des Tickets

GL	CloseDateTime	dateTime	Das Datum/die Uhrzeit, als das Ticket geschlossen wurde
AGLU	OrgID	decimal	Eindeutiger Identifikator der mit dem Ticket verknüpften Organisation
AGLU	OrganizationName	string	Der Name der mit dem Ticket verknüpften Organisation
AGLU	Organization	string	Die mit dem Ticket verknüpfte Organisations-ID
AGLU	OrganizationStaffName	string	Der Name des mit dem Ticket verknüpften Organisationsmitarbeiters
AGLU	OrganizationStaff	string	Die eindeutige ID des mit dem Ticket verknüpften Organisationsmitarbeiters
AGLU	OrganizationStaffEmail	string	Die E-Mail-Adresse des mit dem Ticket verknüpften Organisationsmitarbeiters
AGLU	Machine	string	Der mit dem Ticket verknüpfte Rechner
AGLU	MachineGuid	decimal	Die GUID des mit dem Ticket verknüpften Rechners
AGLU	MachineGroup	string	Die Rechnergruppe des mit dem Ticket verknüpften Rechners
AGLU	MachineGroupGuid	decimal	Die GUID der mit dem Ticket verknüpften Rechnergruppe
AGLU	Submitter	string	Der Name des Absenders, der das Ticket übermittelte
AGLU	SubmitterEmail	string	Die E-Mail-Adresse des Ticketabsenders
AGLU	SubmitterPhone	string	Die Telefonnummer des Ticketabsenders
AGLU	SubmitterType	string	Der Typ der Person, die das Ticket übermittelt: • UNBEKANNT • TEILNEHMER – Ein Teilnehmer ist ein VSA-Benutzer. • BENUTZER – Eine dem VSA unbekannte Person
GL	IsUnread	boolean	Wenn wahr, wurde das Ticket noch nicht vom gegenwärtig angemeldeten Benutzer angezeigt

Vorfall

Der **Incident** wird von **IncidentSummary** abgeleitet und enthält zusätzlich zu den folgenden Feldern auch alle Felder des **IncidentSummary**.

G	IsParticipant	boolean	Veraltet
G	IsClosed	boolean	Wahr, wenn geschlossen
G	CurrentStageEscalation DateTime	dateTime	Datum und Uhrzeit der Phaseneskalation
G	CurrentGoalDateTime	dateTime	Datum und Uhrzeit des Phasenziels
AGU	Owner	string	Eigentümer des Tickets
	Participant	string	Veraltet
AGU	AssigneeType	string	Typ des Administrators: • UNBEKANNT • TEILNEHMER – Einzelner Administrator • POOL – Ein Pool von Benutzern
AGU	Assignee	string	Name des Administrators
AGU	AssigneeEmail	string	E-Mail-Adresse des Administrators
G	ActualCompletionDate	dateTime	Veraltet
G	ExpectedCompletion Date	dateTime	Datum und Uhrzeit, an dem/zu der das Ticket geschlossen wird oder voraussichtlich geschlossen wird (das Fälligkeitsdatum des Ticketziels)

G	ActualResolutionDate	dateTime	Datum und Uhrzeit, an dem/zu der ein Auflösungstyp für das Ticket eingestellt wurde
AGU	PromisedDate	dateTime	Datum, Uhrzeit und versprochenes Datum, das/die vom Kundenrepräsentanten zum Auflösen des Tickets eingegeben wurden
G	IsArchived	boolean	Wahr, wenn das Ticket archiviert wurde
G	IsError	boolean	Veraltet
G	IsPoolAssignee	boolean	Veraltet
	ErrorMessage	string	Veraltet
	Notify	boolean	Veraltet
G	CurrentStage	string	Die aktuelle Phase
AGU	ResolutionNote	string	Beschreibender Text, der mit dem Auflösungstyp eingegeben wurde
G	LockTime	dateTime	Datum und Uhrzeit, an dem/zu der das Ticket gesperrt wurde, indem es zu Bearbeitung geöffnet wurde
G	LockUser	string	Benutzer, der das Ticket sperrte, indem er es zur Bearbeitung öffnete
G	StageGoalTime Remaining	int	Die verbleibende Zeit, bevor der Phasenzielzeitgeber das Zielverfahren ausführt. Relevant, wenn das Phasenziel angehalten wurde.
AGU	SourceType	string	Der Quellentyp, entweder ein Systemereignis oder eine E-Mail-Nachricht, das/die eine Ticketanforderung erzeugte • E-Mail • Backup • KES • Patch • Monitor • Alarm • Portal • Service-Desk • Andere
	OrgAddress/Address	string	Adresse 1 der Organisation
	OrgAddress/Address	string	Adresse 2 der Organisation
	OrgAddress/City	string	Ort der Organisation
	OrgAddress/State	string	Bundesland/Kanton der Organisation
	OrgAddress/Zip	string	Postleitzahl der Organisation
	OrgAddress/Country	string	Adresse der Organisation
AGLU	Field	CustomField	Kein oder mehrere Werte für benutzerdefinierte Felder
AGU	Notes	Note	Keine oder mehrere Anmerkungen
AGU	Attachments	Attachment	Keine oder mehrere Anhänge
AGU	RelatedIncidents	Related Incident	Keine oder mehrere verwandte Vorfälle
	StartDate	datetime	Datum und -uhrzeit des Aufgabenbeginns
	EndDate	datetime	Datum und -uhrzeit des Aufgabenendes
	UpdateTime	datetime	Datum und Uhrzeit der Aufgabenaktualisierung

	FollowupDate	datetime	Datum und Uhrzeit für Follow-up-Aktionen dieser Aufgabe
	CompletionDate	datetime	Datum und Uhrzeit des Aufgabenabschlusses
	ApprovalDate	datetime	Datum und Uhrzeit der Aufgabengenehmigung
	PromiseDate	datetime	Datum und Uhrzeit des zugesagten Aufgabenabschlusses
	PercentCompletion	int	Abschlussprozent der Aufgabe
	TaskStatus	string	Status der Aufgabe
	ActualHours	double	Insgesamt aufgewendete Arbeitsstunden für diese Aufgabe
	Resource	Resource	Keine oder mehrere Ressourcen
	Assignee	string	Der Aufgabe zugewiesene Bearbeiter
	EstimatedHours	decimal	Geschätzte insgesamt aufgewendete Arbeitsstunden für dieses Ticket
	TotalHours	decimal	Tatsächliche insgesamt aufgewendete Arbeitsstunden für dieses Ticket
	PreviousStage	string	Vorige Phase des Tickets
	WorkPerformedDateTime	datetime	Datum und Uhrzeit der letzten Arbeit an diesem Ticket
	EditingTemplate	string	Bearbeitungsvorlage zur Bearbeitung dieses Tickets
GU	ServiceDeskDefinition	ServiceDesk Definition	

KSD-API-Webdienst – Vorgänge

Die folgenden Vorgänge können mit dem **KSD-API-Webdienst** durchgeführt werden.

AddIncident

Die Anforderung lautet:

AddSDIncident	Incident	Der Inhalt des zu erstellenden neuen Vorfalls. Nur Felder, die mit einem "A" in der ersten Spalte markiert sind, können eingestellt werden.
SessionId	Decimal	Die ID der Webdienstsitzung

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

IncidentNumber	string	Der eindeutige Identifikator des Tickets
IncidentID	decimal	Der Identifikator des Tickets
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

AddServDeskToScope

Die Anforderung lautet:

servDeskName	string	Der Name des Service-Desks
scopeName	string	Der Name des Umfangs

SessionId	decimal	Die ID der Webdienstsitzung

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetIncident

Ruft einen einzelnen Vorfall aus der Datenbank ab. Die Anforderung lautet:

IncidentRequest		Der abzurufende Vorfall. Dies bietet die folgenden Felder: • `IncidentNumber` – Die Ticket-ID, wie sie dem Benutzer angezeigt wird, z. B. STD000001 • `IncidentId` – Die Datenbank-ID des abzurufenden Tickets • `IncludeNotes` – Wahr, um Anmerkungen in das abgerufene Ticket aufzunehmen • `IncludeDefinition` – Wahr, um die Service-Desk-Definition in die Antwort aufzunehmen • `IncludeAttachment` – Wahr, um Anhänge in das abgerufene Ticket aufzunehmen
SessionId	Decimal	Die ID der Webdienstsitzung

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

IncidentResponse	Incident	Der abgerufene Vorfall
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetIncidentList

Ruft eine Liste der Vorfälle ab, die mit den Anfragekriterien übereinstimmen.
Die Anforderung lautet:

IncidentRequest		Der abzurufende Vorfall. Dies bietet die folgenden Felder: • `ServiceDeskName` – Der Name des abzufragenden Service-Desks • `Status` – Ein oder mehrere Status, die abgerufen werden sollen. Wenn keine Status angegeben werden, werden die Tickets ungeachtet ihres Status abgerufen. • `Priority` – Ein oder mehrere Prioritätswert(e), der/die abgerufen werden soll(en). Wenn keine Prioritätswerte angegeben werden, werden die Ticket ungeachtet der Priorität abgerufen. • `Stage` – Ein oder mehrere Phasenwert(e), der/die abgerufen werden soll(en). Wenn keine Phasenwerte angegeben werden, werden die Ticket ungeachtet der Phase abgerufen. • `SummarySearch` – Eine Zeichenfolge oder ein Ausdruck für

		einen Suchvorgang in der Ticketübersicht • `Organization` – Der Name oder Teilname von Organisationen, der abgerufen werden soll Wenn keiner angegeben wird, werden Tickets für alle Organisationen im Umfang abgerufen. • `OrganizationStaff` – Der Name eines mit Tickets verknüpften Organisationsmitarbeiters Wenn keiner angegeben wird, werden Tickets für alle Organisationen im Umfang abgerufen. • `Machine` – Der Name eines Rechners, der abgerufen werden soll Wenn keiner angegeben wird, werden Tickets für alle Rechner im Umfang abgerufen. • `MachineGroup` – Der Name einer Rechnergruppe, die abgerufen werden soll Wenn keiner angegeben wird, werden Tickets für alle Rechnergruppen im Umfang abgerufen. • `Assignee` – Die Namen oder Teilnamen von Bearbeitern, die abgerufen werden sollen Wenn keiner angegeben wird, werden Tickets für alle Administratoren im Umfang abgerufen. • `StartingIncident` – Die nächste abzurufende Vorfallnummer beim Seitenwechsel Dieser Wert stammt aus dem Wert "nextStartingIncident" einer vorherigen GetIncidentList-Anforderung. • `IncidentCount` – Wenn vorhanden, gibt dies die Anzahl der abzurufenden Vorfälle an. • `SortField` – Wenn vorhanden, werden die Ergebnisse für den Feldnamen sortiert.
SessionId	Decimal	Die ID der Webdienstsitzung

Die Antwort lautet folgendermaßen:

IncidentList		Die Liste der übereinstimmenden Vorfälle. Dies bietet die folgenden Attribute und Elemente: • `totalIncidents` – Die Gesamtzahl der Vorfälle, die mit der Anforderung übereinstimmen • `nextStartingIncident` – Die ID des nächsten abzurufenden Vorfalls • `Incident` – Kein oder mehrere mit den Anforderungskriterien übereinstimmende(r) Vorfall/Vorfälle
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetIncident2

Gibt alle Werte in GetIncidentList sowie die benutzerdefinierten Felder und Werte pro Vorfall zurück. Weitere Informationen finden Sie unter **GetIncidentList** *(siehe 595)*.

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben.

CustomFields	string or null	Der Wert des benutzerdefinierten Felds wurde in der Anfrage angegeben.

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetServiceDesk

Ruft die Definition eines Service-Desks ab. Diese sollte vor dem Erstellen einer Benutzeroberfläche abgerufen werden, damit der Benutzer ein Ticket eingeben kann. Die Anforderung lautet:

ServiceDeskDefinitionRequest		Das abzurufende Service-Desk. Dies hat die folgenden Elemente: • ServiceDeskName – Der Name des abzurufenden Service-Desks • ServiceDeskID – Die Datenbank des abzurufenden Service-Desks. Sollte nicht verwendet werden.
SessionId	Decimal	Die ID der Webdienstsitzung

Es wird ein einzelner Datensatz der folgenden Elemente zurückgegeben.

ServiceDeskDefinitionResponse	ServiceDeskDefinition	Die abgerufene Desk-Definition
Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

GetServiceDesks

Falls zutreffend, werden mehrere Datensätze der folgenden Felder zurückgegeben. Die Anforderung lautet:

IsDefault	boolean	Wenn wahr, ist das Service-Desk das Standard-Service-Desk.
ServiceDeskID	decimal	Ein eindeutiger Identifikator
ServiceDeskName	string	Der Name des Service-Desks

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Primitive

Darüber hinaus werden die folgenden primitiven Datentypvorgänge durchgeführt. Jeder primitive Vorgang verwendet den gleichen xml-Vertrag wie der entsprechende Mehrspaltenvorgang. Jeder primitive Vorgang gibt einen Zeichenfolgenwert zurück, der weiterer Verarbeitung bedarf. Es wird empfohlen, diese Methoden NICHT zu verwenden.

Primitive	Ergebnis	Datentyp
PrimitiveAddIncident	PrimitiveAddIncidentResult	string
PrimitiveAddServDeskToScope	PrimitiveAddServDeskToScopeResult	string
PrimitiveGetIncident	PrimitiveGetIncidentResult	string
PrimitiveGetIncidentList	PrimitiveGetIncidentListResult	string
PrimitiveGetServiceDesk	PrimitiveGetServiceDeskResult	string
PrimitiveGetServiceDesks	PrimitiveGetServiceDesksResult	string
PrimitiveUpdateIncident	PrimitiveUpdateIncidentResult	string

QueueAddIncident

Stellt eine **AddIncident** *(siehe 594)*-Anfrage in die Warteschlange. Dies wird normalerweise in Situationen verwendet, in denen in kurzer Zeit über die API große Ticketmengen erstellt werden und ein System-Timeout verhindert werden soll. Die Anfrage zum Hinzufügen eines Vorfalls wird einer Tabelle hinzufügt. Ein laufendes Ereignis bezieht sich zur Erstellung von Tickets auf diese Tabelle, sodass die Anfrage nicht auf die Erstellung des Tickets warten muss.

Die Anforderung lautet:

AddSDIncident	Incident	Der hinzuzufügende Vorfall.
SessionId	Decimal	Die ID der Webdienstsitzung

Ein einzelner Datensatz der folgenden Felder wird zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

UpdateIncident

Aktualisiert einen einzelnen Vorfall in der Datenbank. Die Anforderung lautet:

UpdateSDIncident	Incident	Der zu aktualisierende Vorfall. Die Felder, die bei der Aktualisierung gültig sind, können Sie aus der ersten Spalte des Incident-Datentyps ersehen.
SessionId	Decimal	Die ID der Webdienstsitzung

Es wird ein einzelner Datensatz der folgenden Felder zurückgegeben.

Method	string	Der Vorgang, der diese Antwort anforderte
TransactionID	decimal	Die eindeutige Nachrichten-ID dieser Nachricht
ErrorMessage	string	Wenn leer, wurde kein Fehler zurückgegeben
ErrorLocation	string	Wenn leer, wurde kein Fehler zurückgegeben

Probenachrichten

In den folgenden XML-Dateien sind Probedaten enthalten.

GetServiceDesks Request


```
<GetServiceDesks xmlns="vsaServiceDeskWS">
  <req>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetServiceDesks>
```


GetServiceDesks Response


```
<GetServiceDesksResponse xmlns="vsaServiceDeskWS">
  <GetServiceDesksResult>
    <ServiceDesks>
      <ServiceDesk>
        <IsDefault>false</IsDefault>
        <ServiceDeskID>291273277175176</ServiceDeskID>
        <ServiceDeskName>KnowledgeBase</ServiceDeskName>
      </ServiceDesk>
      <ServiceDesk>
        <IsDefault>false</IsDefault>
        <ServiceDeskID>696191121914314</ServiceDeskID>
        <ServiceDeskName>Standard</ServiceDeskName>
      </ServiceDesk>
    </ServiceDesks>
    <Method>GetServiceDesks</Method>
    <TransactionID>144</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetServiceDesksResult>
</GetServiceDesksResponse>
```


GetServiceDesk Request


```
<GetServiceDesk xmlns="vsaServiceDeskWS">
  <req>
    <ServiceDeskDefinitionRequest>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName>
      <ServiceDeskID
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">696191121914314</ServiceDeskID>
    </ServiceDeskDefinitionRequest>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetServiceDesk>
```


GetServiceDesk Response


```
<GetServiceDeskResponse xmlns="vsaServiceDeskWS">
  <GetServiceDeskResult>
    <ServiceDeskDefinitionResponse id="696191121914314">
      <Name xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</Name>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard
SD</Description>
      <RequireTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</RequireTime>
      <DisplayMachineInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</DisplayMachineInfo>
      <RequireMachineInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</RequireMachineInfo>
      <DisplayOrgInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</DisplayOrgInfo>
      <RequireOrgInfo
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</RequireOrgInfo>
      <DisplayCI xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</DisplayCI>
      <RequireCI xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</RequireCI>
      <AllAdmins xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</AllAdmins>
```

```
      <AutoStartClock
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</AutoStartClock>
      <AutoSaveClock
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</AutoSaveClock>
      <AutoInsertNote
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</AutoInsertNote>
      <AutoInsertNoteHidden
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</AutoInsertNoteHidden>
      <NeedStatusNote
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</NeedStatusNote>
      <SDPrefix xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD</SDPrefix>
      <DefaultStatus
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">218924116119912</DefaultStatus>
      <DefaultStage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">831768438118427</DefaultStage>
      <DefaultPriority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">693719171716599</DefaultPriority>
      <DefaultSeverity
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultSeverity>
      <DefaultResolution
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultResolution>
      <DefaultCategory
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">0</DefaultCategory>
      <DefaultServiceDesk
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</DefaultServiceDesk>
      <TemplateType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">1</TemplateType>
      <SequenceName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">SEQ129</SequenceName>
      <EditingTemplate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Fixed_Width_Tabbed.xml</EditingTe
mplate>
      <Status xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Item ref="Standard||AwaitingHardware" id="541491145218711">Awaiting Hardware</Item>
        <Item ref="Standard||AwaitingUserFeedback" id="281767467828324">Awaiting User Feedback</Item>
        <Item ref="Standard||Closed" id="989295147216226">Closed</Item>
        <Item ref="Standard||Escalated" id="551271771474242">Escalated</Item>
        <Item ref="Standard||Hold" id="172151822788151">Hold</Item>
        <Item ref="Standard||InProgress" id="111313126312233">In Progress</Item>
        <Item ref="Standard||New" id="218924116119912">New</Item>
      </Status>
      <Priority xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Item ref="Standard||CriticalHigh" id="744512181719881">Critical High</Item>
        <Item ref="Standard||High" id="982525519923522">High</Item>
        <Item ref="Standard||Low" id="291721863176342">Low</Item>
        <Item ref="Standard||Medium" id="693719171716599">Medium</Item>
        <Item ref="Standard||Planning" id="176222131631332">Planning</Item>
      </Priority>
      <Severity xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Item ref="Standard||CompanyWide(High)" id="315477225242249">Whole Company (High)</Item>
        <Item ref="Standard||MultipleUsers(Medium)" id="262164368749722">Multiple users (Medium)</Item>
        <Item ref="Standard||OneUser(Low)" id="917688316816914">Single User (Low)</Item>
      </Severity>
      <Resolution xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Item ref="Standard||AdviceGiven" id="498162732192611">Advice Given</Item>
        <Item ref="Standard||CannotDuplicate" id="262514419248621">Cannot Duplicate</Item>
        <Item ref="Standard||ClosedbyCustomerRequest" id="525192125718333">Closed by Customer
Request</Item>
        <Item ref="Standard||HardwareReplaced" id="432262321578326">Hardware Replaced</Item>
        <Item ref="Standard||HotFixReleased" id="189239616133249">Hot Fix Released</Item>
        <Item ref="Standard||InstallationCompleted" id="139764799836252">Installation Completed</Item>
        <Item ref="Standard||NewSoftwareInstalled" id="521637923418319">New Software Installed</Item>
        <Item ref="Standard||Noresponsefromuser" id="115424612244857">No response from user</Item>
        <Item ref="Standard||OSReinstalled" id="531617444692623">OS Reinstalled</Item>
        <Item ref="Standard||Other" id="711261961631328">Other</Item>
        <Item ref="Standard||PassedtoSales" id="191482475814123">Passed to Sales</Item>
        <Item ref="Standard||Pendingscriptcleared" id="762515513181192">Pending script cleared</Item>
        <Item ref="Standard||ReapplySchema" id="525317525441497">Reapply Schema</Item>
        <Item ref="Standard||Reboot" id="832182442825238">Reboot</Item>
```

```
        <Item ref="Standard||ResolvedbyCustomer" id="243623591961272">Resolved by Customer</Item>
        <Item ref="Standard||ResolvedbyTechnition" id="423939164212169">Resolved</Item>
        <Item ref="Standard||SolvedwithKBarticle" id="272199179212412">Solved with KB article</Item>
        <Item ref="Standard||TrainingGiven" id="622224812237126">Training Given</Item>
      </Resolution>
      <Categories xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Category>
          <Item ref="Standard||Advice&amp;Guidance" id="161211171768212">Advice &amp; Guidance</Item>
          <SubCategory ref="Standard||Advice&amp;Guidance||General"
id="561699795215782">General</SubCategory>
        </Category>
        <Category>
          <Item ref="Standard||Kaseya" id="641881726251641">Kaseya</Item>
          <SubCategory ref="Standard||Kaseya||AgentIcon" id="821781865922435">Agent Icon</SubCategory>
          <SubCategory ref="Standard||Kaseya||Alarm" id="481422361723261">Alarm</SubCategory>
          <SubCategory ref="Standard||Kaseya||ApplicationChanges" id="525187874623717">Application
Changes</SubCategory>
          <SubCategory ref="Standard||Kaseya||Disk" id="919621482151882">Disk</SubCategory>
          <SubCategory ref="Standard||Kaseya||Eventlog" id="814714713317798">Eventlog</SubCategory>
          <SubCategory ref="Standard||Kaseya||GetFile" id="322618792314914">Get File</SubCategory>
          <SubCategory ref="Standard||Kaseya||Hardware" id="176166136238942">Hardware</SubCategory>
          <SubCategory ref="Standard||Kaseya||Lanwatch" id="214791394922624">Lanwatch</SubCategory>
          <SubCategory ref="Standard||Kaseya||Logon_Admin"
id="943315515116292">Logon_Admin</SubCategory>
          <SubCategory ref="Standard||Kaseya||Logon_User"
id="636613429245187">Logon_User</SubCategory>
          <SubCategory ref="Standard||Kaseya||NewAgent" id="557214511134217">New Agent</SubCategory>
          <SubCategory ref="Standard||Kaseya||Other" id="631281678197153">Other</SubCategory>
          <SubCategory ref="Standard||Kaseya||PatchManagement" id="462824113621914">Patch
Management</SubCategory>
          <SubCategory ref="Standard||Kaseya||Procedure" id="274262311559714">Procedure</SubCategory>
          <SubCategory ref="Standard||Kaseya||RCDisabled" id="641624812335116">RC
Disabled</SubCategory>
          <SubCategory ref="Standard||Kaseya||Script" id="471482131991414">Script</SubCategory>
          <SubCategory ref="Standard||Kaseya||SystemOffline" id="113411182222324">System
Offline</SubCategory>
          <SubCategory ref="Standard||Kaseya||SystemOnline" id="251814418923368">System
Online</SubCategory>
          <SubCategory ref="Standard||Kaseya||Unidentified"
id="617313577253122">Unidentified</SubCategory>
        </Category>
        <Category>
          <Item ref="Standard||Network" id="414766231875111">Network</Item>
          <SubCategory ref="Standard||Network||Connectivity"
id="122145211361321">Connectivity</SubCategory>
          <SubCategory ref="Standard||Network||Design" id="495611529142242">Design</SubCategory>
          <SubCategory ref="Standard||Network||Firewall" id="812515316323522">Firewall</SubCategory>
          <SubCategory ref="Standard||Network||Other" id="946227769167531">Other</SubCategory>
          <SubCategory ref="Standard||Network||Performance"
id="941891772111717">Performance</SubCategory>
        </Category>
        <Category>
          <Item ref="Standard||Printer" id="155243642251342">Printer</Item>
          <SubCategory ref="Standard||Printer||Other" id="341431321188813">Other</SubCategory>
          <SubCategory ref="Standard||Printer||PrinterProblem" id="851831547314111">Printer
Problem</SubCategory>
          <SubCategory ref="Standard||Printer||PrinterSetup" id="619395216749723">Printer
Setup</SubCategory>
          <SubCategory ref="Standard||Printer||Toner" id="161984536861723">Toner</SubCategory>
        </Category>
        <Category>
          <Item ref="Standard||ServiceRequest" id="541124124415221">Service Request</Item>
          <SubCategory ref="Standard||ServiceRequest||EquipmentMove" id="862712311517672">Equipment
Move</SubCategory>
          <SubCategory ref="Standard||ServiceRequest||NewLaptop" id="266812518245792">New
Laptop</SubCategory>
          <SubCategory ref="Standard||ServiceRequest||NewServer" id="322872913227349">New
Server</SubCategory>
          <SubCategory ref="Standard||ServiceRequest||NewWorkstation" id="224115236352441">New
```

```
Workstation</SubCategory>
        </Category>
      </Categories>
      <Stages xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Stage stageType="End">
          <Item ref="Standard||Closed" id="213813735111171" description="Auto Generated">Closed</Item>
          <Initialization>Standard Enters Closed</Initialization>
        </Stage>
        <Stage stageType="Begin">
          <Item ref="Standard||Identified" id="831768438118427" description="New ticket is
received">Identified</Item>
          <Initialization>Standard Enters Identified</Initialization>
          <Escalation time="15" unit="MINUTE">Incident is Escalated</Escalation>
          <Goal time="1" unit="HOUR">Identified Goal</Goal>
          <NextStage ref="Standard||Tier1" id="546812745461511" description="Tier 1
Support">Tier1</NextStage>
        </Stage>
        <Stage stageType="Middle">
          <Item ref="Standard||Tier1" id="546812745461511" description="Tier 1 Support">Tier1</Item>
          <Initialization>Standard Enters Tier1</Initialization>
          <Escalation time="3" unit="HOUR">Incident is Escalated</Escalation>
          <Goal time="2" unit="HOUR">Tier1 Goal</Goal>
          <NextStage ref="Standard||Closed" id="213813735111171" description="Auto
Generated">Closed</NextStage>
          <NextStage ref="Standard||Tier2" id="318527191192719" description="Tier 2 Specialist
Support">Tier2</NextStage>
        </Stage>
        <Stage stageType="Middle">
          <Item ref="Standard||Tier2" id="318527191192719" description="Tier 2 Specialist
Support">Tier2</Item>
          <Initialization>Standard Enters Tier2</Initialization>
          <Escalation time="3" unit="HOUR">Incident is Escalated</Escalation>
          <Goal time="4" unit="HOUR">Tier2 Goal</Goal>
          <NextStage ref="Standard||Closed" id="213813735111171" description="Auto
Generated">Closed</NextStage>
        </Stage>
      </Stages>
      <Participants xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Participant ref="garyw" id="67511883639135112891416313" isPool="false">garyw</Participant>
        <Participant ref="jschenck" id="72381729521421633172123416"
isPool="false">jschenck</Participant>
        <Participant ref="NickT" id="96171921315349923924634249" isPool="false">NickT</Participant>
        <Participant ref="Standard||SupportManager" id="654222596258293" isPool="true">SupportManager
(Pool)</Participant>
        <Participant ref="Standard||Tier1Support" id="352161952139188" isPool="true">Tier1Support
(Pool)</Participant>
        <Participant ref="Standard||Tier2Support" id="921522231318131" isPool="true">Tier2Support
(Pool)</Participant>
      </Participants>
      <CustomFields xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Field id="221552971661261">
          <Caption>Source</Caption>
          <Title>Source</Title>
          <FieldName>Source</FieldName>
          <FieldFormat>List</FieldFormat>
          <DefaultValue>Call</DefaultValue>
          <Values>
            <Item ref="Call" id="0">Call</Item>
            <Item ref="EMail" id="0">EMail</Item>
            <Item ref="Text" id="0">Text</Item>
          </Values>
        </Field>
        <Field id="818831117157241">
          <Caption>Urgency</Caption>
          <Title>Urgency</Title>
          <FieldName>Urgency</FieldName>
          <FieldFormat>List</FieldFormat>
          <DefaultValue>Medium</DefaultValue>
          <Values>
```

```
        <Item ref="High" id="0">High</Item>
        <Item ref="Low" id="0">Low</Item>
        <Item ref="Medium" id="0">Medium</Item>
      </Values>
    </Field>
    <Field id="513119818455188">
      <Caption>KB Article created</Caption>
      <Title>KB Article Created</Title>
      <FieldName>KB_Article</FieldName>
      <FieldFormat>List</FieldFormat>
      <DefaultValue>No</DefaultValue>
      <Values>
        <Item ref="No" id="0">No</Item>
        <Item ref="Yes" id="0">Yes</Item>
      </Values>
    </Field>
    <Field id="291214644251233">
      <Caption>Dept</Caption>
      <Title>Department</Title>
      <FieldName>Dept</FieldName>
      <FieldFormat>List</FieldFormat>
      <DefaultValue>IT</DefaultValue>
      <Values>
        <Item ref="Accounting" id="0">Accounting</Item>
        <Item ref="Accounts Payable" id="0">Accounts Payable</Item>
        <Item ref="Facilities" id="0">Facilities</Item>
        <Item ref="HR" id="0">HR</Item>
        <Item ref="IT" id="0">IT</Item>
        <Item ref="Other" id="0">Other</Item>
        <Item ref="Payroll" id="0">Payroll</Item>
        <Item ref="Sales" id="0">Sales</Item>
        <Item ref="Telecom" id="0">Telecom</Item>
      </Values>
    </Field>
  </CustomFields>
  <AccessRights xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    <ViewHiddenNotes>true</ViewHiddenNotes>
    <ChangeHiddenNotes>true</ChangeHiddenNotes>
    <FieldRights>
      <FieldRight>
        <FieldName>ID</FieldName>
        <AccessType>Required</AccessType>
      </FieldRight>
      <FieldRight>
        <FieldName>Summary</FieldName>
        <AccessType>Required</AccessType>
      </FieldRight>
      <FieldRight>
        <FieldName>Description</FieldName>
        <AccessType>Edit</AccessType>
      </FieldRight>
      <FieldRight>
        <FieldName>CreationDtTm</FieldName>
        <AccessType>ViewOnly</AccessType>
      </FieldRight>
      <FieldRight>
        <FieldName>SubmitterName</FieldName>
        <AccessType>Edit</AccessType>
      </FieldRight>
      <FieldRight>
        <FieldName>SubmitterEmailAddr</FieldName>
        <AccessType>Edit</AccessType>
      </FieldRight>
      <FieldRight>
        <FieldName>ContactPhone</FieldName>
        <AccessType>Edit</AccessType>
      </FieldRight>
      <FieldRight>
        <FieldName>OrgName</FieldName>
```

```
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>OrgID</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>StaffID</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>ContactEmail</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>MachineID</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>Note</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>ClosedDtTm</FieldName>
    <AccessType>ViewOnly</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>PromiseDtTm</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>DueDtTm</FieldName>
    <AccessType>ViewOnly</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>ActualCompletedDate</FieldName>
    <AccessType>ViewOnly</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>HiddenNote</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>Owner</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>LockUser</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>EditDtTm</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>current_esc_datetime</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>current_goal_datetime</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>lockTime</FieldName>
    <AccessType>Edit</AccessType>
  </FieldRight>
  <FieldRight>
    <FieldName>sourceType</FieldName>
    <AccessType>Edit</AccessType>
```

```
          </FieldRight>
          <FieldRight>
            <FieldName>Status</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Priority</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Severity</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Category</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>SubCategory</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Stage</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Resolution</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Assignee</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Source</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Urgency</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>KB_Article</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
          <FieldRight>
            <FieldName>Dept</FieldName>
            <AccessType>Edit</AccessType>
          </FieldRight>
        </FieldRights>
      </AccessRights>
      <NoteTemplates xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Item ref="My Note" id="196429316815241">My Note</Item>
        <Item ref="Note 2" id="167218821431219">Second note</Item>
      </NoteTemplates>
      <ChangeProcedure xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard is
Changed</ChangeProcedure>
      <GoalProcedure time="1" unit="DAY"
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard Goal - All
Stages</GoalProcedure>
    </ServiceDeskDefinitionResponse>
    <Method>GetServiceDesk</Method>
    <TransactionID>146</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetServiceDeskResult>
</GetServiceDeskResponse>
```

GetIncidentList Request

```
<GetIncidentList xmlns="vsaServiceDeskWS">
  <req>
    <IncidentListRequest>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName>
      <IncidentCount
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">30</IncidentCount>
    </IncidentListRequest>
    <SessionID>62648424383576321292545755</SessionID>
  </req>
</GetIncidentList>
```

GetIncidentList Response

```
<GetIncidentListResponse xmlns="vsaServiceDeskWS">
  <GetIncidentListResult>
    <IncidentList>
      <Incident xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <ServiceDeskName>Standard</ServiceDeskName>
        <IncidentNumber>STD000001</IncidentNumber>
        <Summary>Getting Started with Service Desk - PLEASE READ!</Summary>
        <Status>Closed</Status>
        <Priority>Low</Priority>
        <Stage>Closed</Stage>
        <CreateDateTime>2010-02-05T17:07:21.55-08:00</CreateDateTime>
        <LastEditDateTime>2010-02-05T22:59:22.64-08:00</LastEditDateTime>
        <Submitter>Kaseya Support</Submitter>
        <SubmitterEmail>noreply@kaseya.com</SubmitterEmail>
      </Incident>
    </IncidentList>
    <Method>GetIncidentList</Method>
    <TransactionID>147</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </GetIncidentListResult>
</GetIncidentListResponse>
```

GetIncident Request

```
<GetIncident xmlns="vsaServiceDeskWS">
  <req>
    <IncidentRequest>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000001</IncidentNumber>
      <IncludeNotes
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IncludeNotes>
      <IncludeDefinition
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IncludeDefinition>
    </IncidentRequest>
    <SessionID>67223225114316912673490269</SessionID>
  </req>
</GetIncident>
```

GetIncident Response

```
<GetIncidentResponse xmlns="vsaServiceDeskWS">
  <GetIncidentResult>
    <IncidentResponse id="611922114996841">
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000001</IncidentNumber>
      <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Getting Started with
Service Desk - PLEASE READ!</Summary>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
    &lt;p&gt;&lt;strong&gt;&lt;span
style='font-size:11.0pt;font-family:"Calibri","sans-serif";color:blue'&gt;WELCOME TO SERVICE
```

```
DESK&lt;/span&gt;&lt;/strong&gt;&lt;br/&gt;
    Your Service Desk module has been pre-configured with a template-driven Standard service desk, and
a Knowledge Base desk. Only a few short customization steps are required to use these desks immediately.
See &lt;a href="http://help.kaseya.com/WebHelp/EN/KSD/1000000/index.htm?toc.htm?5982.htm"&gt;Getting
Started&lt;/a&gt; to quickstart your implementation of Service Desk.
    &lt;/p&gt;
  </Description>
      <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Closed</Status>
      <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Low</Priority>
      <Stage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Closed</Stage>
      <Category
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Advice&amp;Guidance</Ca
tegory>
      <CreateDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T17:07:21.55-08:00</Cre
ateDateTime>
      <LastEditDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T22:59:22.64-08:00</Las
tEditDateTime>
      <Submitter xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Kaseya
Support</Submitter>
      <SubmitterEmail
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">noreply@kaseya.com</SubmitterEmai
l>
      <SubmitterType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">UNKNOWN</SubmitterType>
      <IsUnread xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IsUnread>
      <IsParticipant
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsParticipant>
      <Owner xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Owner>
      <AssigneeType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">POOL</AssigneeType>
      <Assignee
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Tier1Support</Assignee>
      <ActualCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-05T22:59:29.28-08:00</Act
ualCompletionDate>
      <ExpectedCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-02-06T17:07:22.283-08:00</Ex
pectedCompletionDate>
      <IsArchived
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsArchived>
      <IsError xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsError>
      <Notify xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</Notify>
      <SourceType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">ServiceDesk</SourceType>
      <CustomFields xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Field fieldName="Source">Text</Field>
        <Field fieldName="Urgency">Low</Field>
        <Field fieldName="KB_Article">No</Field>
        <Field fieldName="Dept">Sales</Field>
      </CustomFields>
      <Notes xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
        <Note id="213494962391116">
          <Timestamp>2010-02-05T22:59:25.127-08:00</Timestamp>
          <Text>Auto Generated Note:&lt;br/&gt;
Ticket Changed&lt;br/&gt;    'currentStageGoalDateTime' cleared&lt;br/&gt;</Text>
          <Hidden>true</Hidden>
        </Note>
        <Note id="356934215185622">
          <User>garyw</User>
          <Timestamp>2010-02-05T17:07:21.55-08:00</Timestamp>
          <Text>Auto Generated Note:&lt;br/&gt;
Ticket Added&lt;br/&gt;</Text>
          <Hidden>true</Hidden>
        </Note>
```

```
    </Notes>
  </IncidentResponse>
  <Method>GetIncident</Method>
  <TransactionID>200</TransactionID>
  <ErrorMessage/>
  <ErrorLocation/>
 </GetIncidentResult>
</GetIncidentResponse>
```

AddIncident Request

```
<AddIncident xmlns="vsaServiceDeskWS">
  <req>
    <AddSDIncident>
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard</ServiceDeskName>
      <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Test Ticket From Web
Service</Summary>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">This ticket was
created with the web service.</Description>
      <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||New</Status>
      <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Medium</Priority>
      <Category
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Network</Category>
    </AddSDIncident>
    <SessionID>67223225114316912673490269</SessionID>
  </req>
</AddIncident>
```

AddIncident Response

```
<AddIncidentResponse xmlns="vsaServiceDeskWS">
  <AddIncidentResult>
    <AddSDIncidentResponse>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">STD000002</IncidentNumber>
      <IncidentID
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">249259141859248</IncidentID>
    </AddSDIncidentResponse>
    <Method>AddIncident</Method>
    <TransactionID>203</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </AddIncidentResult>
</AddIncidentResponse>
```

Kapitel 14

UpdateIncident Request


```
<UpdateIncident xmlns="vsaServiceDeskWS">
  <req>
    <UpdateSDIncident id="894212819800719301574914 35">
      <ServiceDeskName
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Customer_SD_Basic</ServiceDeskNam
e>
      <IncidentNumber
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">CSN000380</IncidentNumber>
      <Summary xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Test Ticket From Web
Service</Summary>
      <Description xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">This ticket was
created with the web service.</Description>
      <Status
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||InProgress</Status>
      <Priority
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Low</Priority>
      <Stage
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Standard||Identified</Stage>
      <CreateDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:07:31.923-08:00</Cr
eateDateTime>
      <LastEditDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:07:31.923-08:00</La
stEditDateTime>
      <Submitter xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Submitter>
      <SubmitterType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">UNKNOWN</SubmitterType>
      <IsUnread xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">true</IsUnread>
      <IsParticipant
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsParticipant>
      <CurrentStageEscalationDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T21:22:43.063-08:00</Cu
rrentStageEscalationDateTime>
      <CurrentGoalDateTime
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-10T22:07:43.077-08:00</Cu
rrentGoalDateTime>
      <Owner xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">garyw</Owner>
      <AssigneeType
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">POOL</AssigneeType>
      <Assignee
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">Tier1Support</Assignee>
      <ExpectedCompletionDate
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">2010-03-11T21:07:43.077-08:00</Ex
pectedCompletionDate>
      <IsArchived
xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsArchived>
      <IsError xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</IsError>
```

```
        <Notify xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">false</Notify>
        <Notes xmlns="http://www.kaseya.com/vsa/2007/12/ServiceDeskDefinition.xsd">
          <Note id="281273717819319">
            <User>garyw</User>
            <Timestamp>2010-03-10T21:07:31.923-08:00</Timestamp>
            <Text>Auto Generated Note:&lt;br/&gt; Ticket Added&lt;br/&gt;</Text>
            <Hidden>true</Hidden>
          </Note>
        </Notes>
      </UpdateSDIncident>
      <SessionID xmlns="">98782788528483188965186776</SessionID>
    </req>
  </UpdateIncident>
```


UpdateIncident Response


```
<UpdateIncidentResponse xmlns="vsaServiceDeskWS">
  <UpdateIncidentResult>
    <Method>UpdateIncident</Method>
    <TransactionID>205</TransactionID>
    <ErrorMessage/>
    <ErrorLocation/>
  </UpdateIncidentResult>
</UpdateIncidentResponse>
```

Glossar

Active Directory

Bei Active Directory handelt es sich um einen Verzeichnisdienst, mit dem Informationen über die Netzwerkressource in einer gesamten Domain gespeichert werden. Sein Hauptzweck besteht darin, zentrale Authentifizierungs- und Autorisierungsdienste für Windows-basierte Computer bereitzustellen. Eine Active Directory-Struktur ist eine hierarchische Gliederung von Objekten. Die Objekte fallen in drei Hauptkategorien: Ressourcen (z. B. Drucker), Dienste (z. B. E-Mail) und Benutzer (Benutzerkonten und Gruppen). Das AD stellt Informationen über die Objekte bereit, organisiert die Objekte, steuert den Zugriff und bestimmt die Sicherheitsvorkehrungen.

Durch Referenzieren von in Active Directory gespeicherten Informationen kann der VSA Rechner, Kontakte und Benutzer verwalten. Weitere Informationen erhalten Sie im **Discovery**-Modul unter Ermittlung nach Domäne.

Agent-Einstellungen

Mittels des VSA können Sie verschiedene Werte für die folgenden Arten von Agent-Einstellungen auf Rechnerbasis angeben, was für Flexibilität und Automatisierungsmöglichkeiten sorgt:

- **Anmeldedaten** *(siehe 77)*
- **Agent-Menü** *(siehe 66)*
- **Eincheckkontrolle** *(siehe 68)*
- **Arbeitsverzeichnis** *(siehe 72)*
- **Protokolle** *(siehe 36)*
- Rechnerprofil – Verweist auf Einstellungen in Inventarisierung > **Profil bearbeiten** *(siehe 73)*.
- **Sammlungen ansehen** *(siehe 628)*
- **Portalzugriff** *(siehe 75)*
- Remote-Control-Richtlinie
- **Patch-Einstellungen** *(siehe 624)*
- Patchdateiquelle
- Zugehörigkeit zu Patch-Richtlinien
- Festgelegte Meldungen – Alle diese Meldungstypen werden auf der Seite Monitor > **Meldungen** *(siehe 284)* angezeigt, mit Ausnahme von Ereignisprotokoll- und Systemmeldungen.
- **Ereignisprotokoll-Meldungen** *(siehe 284)*
- **Monitor-Sets** *(siehe 267)*
- **Dateien verteilen** *(siehe 135)*
- Schutz
- Geplante Skripte

Agent-Menü

Die Reihe von Optionen, die angezeigt werden, wenn der Benutzer mit der rechten Maustaste auf das Symbol **Agent** *(siehe 611)* in der **Systemablage** *(on seite 631)* des verwalteten Rechners klickt. Das Agent-Menü kann **angepasst** *(siehe 66)* werden.

Agents

Die Verwaltung der Rechner über den VSA erfolgt durch Installieren eines Software-Clients auf einem verwalteten Rechner, der als ein **Agent** bezeichnet wird. Bei dem Agent handelt es sich um einen Systemdienst, bei dem der Benutzer nicht angemeldet sein muss, damit der Agent funktioniert, und der

auch keinen Neustart erfordert, damit der Agent installiert werden kann. Der Agent ist konfigurierbar und kann für den Benutzer völlig unsichtbar sein. Der einzige Zweck des Agents ist es, die vom VSA-Benutzer angeforderten Aufgaben auszuführen. Nach der Installation:

- In der Systemablage des verwalteten Rechners wird ein Agent-Symbol, wie beispielsweise das Agent-Symbol angezeigt. Bei **Agent-Symbolen** *(siehe 24)* kann es sich um benutzerdefinierte Bilder handeln. Sie können jedoch auch ganz entfernt werden.
- Jedem installierten Agent wird eine eindeutige VSA **Rechner-ID/Gruppen-ID/Organisation-ID** *(siehe 626)* zugewiesen. Rechner-IDs können automatisch bei der Installation des Agents oder einzeln vor der Installation des Agents erstellt werden.
- Jeder installierte Agent verbraucht eine der verfügbaren Agent-Lizenzen, die vom Service-Provider erworben wurden.
- Agents werden in der Regel über Pakete installiert, die mit Agent > **Agents bereitstellen** *(siehe 40)* im VSA erstellt werden.
- Auf einem Rechner können **mehrere Agents** *(siehe 50)* installiert werden, die jeweils auf einen anderen Server verweisen.
- Neben jeder Rechner-ID im VSA wird ein **Check-in-Symbol** *(siehe 16)* angezeigt, das den Gesamtstatus des verwalteten Rechners angibt. Das Anmeldsymbol weist beispielsweise darauf hin, dass der Agent online und der Benutzer momentan angemeldet ist.
- Wenn Sie auf ein Anmeldesymbol klicken, wird eine einzelne Rechneroberfläche für den verwalteten Rechner namens **Live-Connect** *(siehe 17)* angezeigt. **Live-Connect** bietet sofortigen Zugriff auf umfassende Daten und Tools, die Sie für das Arbeiten auf diesem spezifischen Rechner benötigen.
- Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt. Über das Agent-Schnellansichtsfenster können Sie ein Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten.

Agents – Apple

Apple-Agents unterstützen die folgenden Funktionen:

- Audits – Ausgewählte Hardware- und Software-Attribute
- Agent-Verfahren
- Remote Control
- FTP
- SSH
- Kennwort zurücksetzen
- Task-Manager
- Live-Connect mit Desktopzugriff.
  - Auf Apple Leopard (Intel) und höher, einschließlich Lion und Mountain Lion, können Sie Desktopzugriff in Live-Connect nutzen, um ein Windows System, das Firefox oder Safari verwendet, remote zu steuern.
  - Unter Verwendung einer unserer unterstützten Browser können Sie unter Windows Desktop-Zugriff verwenden, um Apple Leopard (Intel) und höher, einschließlich Lion und Mountain Lion, remote zu steuern.
- Aufzeichnung der Desktop-Sitzung über Fernsteuerung und Schnellansicht für Snow Leopard und höher, einschließlich Lion und Mountain Lion.
- LAN-Watch über Ermittlung
- Monitoring wurde unterstützt:
  - SNMP-Monitoring
  - Monitoring in Monitor-Sets verarbeiten
  - Systemprüfung
  - Log-Parser

Siehe **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Agents – Linux

Linux Agents unterstützen die folgenden Funktionen:

- Agent-Verfahren
- Letzte Audits, Basis-Audits und System-Audits
- Remote Control und FTP mit VNC
- SSH
- Kennwort zurücksetzen
- LAN-Watch und Agents installieren – Siehe **Linux Agents installieren** *(siehe 52)*.
- Meldungen
- Überwachung der Prozesse
- Überwachung von SNMP
- Log-Parser
- Benutzerspezifische Site-Anpassung – Die Registerkarte **Agent-Symbole** bietet jetzt einen Symbolsatz für Linux Agents, die Sie anpassen können.
- Nur auf bestimmte nicht-pluginfähige Elemente kann über einen Linux-basierten Browser oder beim Browsen auf einen Linux Agent-Rechner zugegriffen werden. Dazu gehören:
- Live-Connect – Nur auf bestimmte nicht-pluginfähige Elemente kann über einen Linux-basierten Browser oder beim Browsen auf einen Linux Agent-Rechner zugegriffen werden. Unterstützte Menüoptionen wie folgt:
  - Startseite
  - Agent-Daten
  - Audit-Information
  - Ticketing (oder Service-Desk-Ticketing)
  - Chat
  - Video-Chat

Siehe **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm)*.

Aktuelle VSA-Zeit

Die vom Kaseya Server verwendete aktuelle Zeit wird unter System > **Voreinstellungen** *(siehe 402)* angezeigt.

Alarme – Aussetzen

Über die Seite **Alarme aussetzen** können Sie **Alarme** *(siehe 622)* für vorgegebene Zeitspannen, einschließlich wiederkehrender Zeitperioden, aussetzen. Dadurch können Sie Aufrüstungs- und Pflegeaufgaben durchführen, ohne einen Alarm auszulösen. Wenn Alarme für eine Rechner-ID ausgesetzt sind, *sammelt der Agent weiterhin Daten, generiert jedoch keine zugehörigen Alarme*.

Analysedefinitionen und Analysesätze

Bei der Konfiguration des **Protokoll-Monitoring** *(siehe 626)* ist es hilfreich, zwischen zwei Arten von Konfigurationsdatensätzen zu unterscheiden: **Analysedefinitionen** und **Analysesätze**.

Eine **Analysedefinition** wird für Folgendes verwendet:

- Ermitteln der zu analysierenden Protokolldatei
- Auswählen der Protokolldaten basierend auf dem *Format* der Protokolldaten, laut Angabe in einer Vorlage
- Ausfüllen der Parameter mit Protokolldatenwerten
- Wahlweise Formatierung des Protokolleintrags in **Protokoll-Monitoring**

Mit einem **Analysesatz** werden die ausgewählten Daten anschließend *gefiltert*. Basierend auf den *Werten* der ausgefüllten Parameter und der definierten Kriterien kann ein Analysesatz

Protokoll-Monitoring-Einträge generieren und optional Meldungen auslösen.

Falls durch den Analysesatz keine Filterung stattfinden würde, würde die Kaseya Server-Datenbank in kürzester Zeit stark anwachsen. Ein Protokolldateiparameter namens $FileServerCapacity$ würde beispielsweise wiederholt mit dem aktuellen Prozentsatz des freien Speicherplatzes auf einem Dateiserver aktualisiert werden. Bis dieser freie Speicherplatz jedoch auf unter 20 % fällt, braucht dies nicht im **Protokoll-Monitoring** aufgezeichnet zu werden und es braucht auch keine Meldung basierend auf diesem Schwellenwert ausgelöst zu werden. Jeder Analysesatz gilt nur für die Analysedefinition, für deren Filterung er erstellt wurde. Für jede Analysedefinition können mehrere Analysesätze erstellt werden. Jeder Analysesatz kann einen separaten Alarm auf jeder Rechner-ID auslösen, der er zugewiesen wurde.

Anmeldedaten

Als Anmeldedaten bezeichnet man den Benutzernamen und das Kennwort, die zur Authentifizierung des Zugriffs auf einen Rechner, ein Netzwerk oder eine andere Ressource durch einen Benutzer oder einen Prozess verwendet werden.

Agent-Anmeldeinformationen

Legen Sie über die Seite Agent > **Anmeldedaten eingeben** *(siehe 77)* einen *einzelnen Satz* von Anmeldeinformationen mit Administratorrechten zur Verwendungen durch einen Agent fest.

Verwaltete Anmeldeinformationen

Geben Sie *zusätzliche* Anmeldedaten auf drei verschiedenen Ebenen an: nach Organisation, nach Rechnergruppe und nach einzelnem Rechner oder Gerät. Sie werden mithilfe von drei Navigationselementen im Modul **Audit** verwaltet:

- **Bestand anzeigen** *(siehe 141)* – Erstellen Sie über diese Seite mehrere Sätze von Anmeldeinformationen für *einzelne* Rechner oder Geräte.
- **Anmeldeinformationen verwalten** *(siehe 144)* – Erstellen Sie über diese Seite mehrere Sätze von Anmeldeinformationen für *Unternehmen* und *Rechnergruppen* innerhalb von Unternehmen.
- **Anmeldeinformationen-Protokolle** *(siehe 146)* – Auf dieser Seite werden die Erstellung, die Anzeige und die Löschung verwalteter Anmeldeinformationen protokolliert.

Verwenden Sie verwaltete Anmeldeinformationen nach ihrer Erstellung zu Folgendem:

- Für die sofortige Suche aller Anmeldeinformationen, die für den Rechner, an dem Sie gerade arbeiten, gelten. Das Popup-Fenster **Schnellanzeige** enthält jetzt die Option **Anmeldeinformationen anzeigen**. Zugriff wird nach Rolle und Bereich gesteuert. Sie können jedem Satz von Anmeldeinformationen eine Beschreibung hinzufügen.
- Als Quell-Anmeldeinformationen für Agent-Anmeldeinformationen in einer Richtlinie. Aktivieren Sie in den Einstellungen **Anmeldedaten** auf der Seite Policy Management > Richtlinien das Kontrollkästchen **Standardeinstellungen von Unternehmen verwenden**, um die Verknüpfung einzurichten.

> **Hinweis:** Die Einstellungen unter Agent > **Anmeldedaten eingeben** *(siehe 77)* können nicht direkt durch verwaltete Anmeldeinformationen überschrieben werden. Verwaltete Anmeldeinformationen müssen auf eine Richtlinie angewendet und diese Richtlinie muss wiederum auf einen Rechner angewendet werden.

Wenn für einen Rechner mehrere Sätze von Anmeldeinformationen definiert sind, hat die lokal am nächsten liegende Ebene Vorrang: nach Einzelrechner, nach Rechnergruppe oder nach Unternehmen. Auf jeder dieser Ebenen kann nur jeweils ein Satz verwalteter Anmeldeinformationen als Quell-Anmeldeinformationen für die Agent-Anmeldeinformationen designiert werden.

Anmeldestatus

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das **Agent-Schnellansichtsfenster** *(siehe 17)* angezeigt.

Online, aber in Wartestellung bis zum Abschluss des ersten Audits
Agent online
Agent online und Benutzer gegenwärtig angemeldet.
Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
Agent ist gegenwärtig offline
Agent hat nie eingecheckt.
Agent ist online, aber die Fernsteuerung wurde deaktiviert.
Agent wurde ausgesetzt.

Ansichtsdefinitionen

Über das Fenster **Definitionen anzeigen** *(siehe 27)* können Sie einen Rechner-ID/Gruppen-ID-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern. Ansichten bieten den Benutzern Flexibilität bei der Verwaltung und Berichterstattung ihrer Rechner. Ansichtsfilterung wird auf *alle* Funktionsseiten angewendet. Hierzu wählen Sie eine Ansicht aus der Dropdown-Liste **Ansicht auswählen** im Bereich **Rechner-ID/Gruppen-ID-Filter** *(siehe 26)* aus und klicken auf das Symbol 'Anwenden' . Es kann eine beliebige Anzahl von Ansichten erstellt und mit anderen Benutzern gemeinsam verwendet werden. Zum Erstellen von Ansichten klicken Sie auf **Bearbeiten** rechts von der Dropdown-Liste **Ansichten**.

Audit

Agents *(siehe 611)* können für eine automatische regelmäßige Inventarisierung der Hardware- und Softwarekonfigurationen ihrer verwalteten Rechner geplant werden. Agents geben die Informationen an den Kaseya Server zurück, sodass Sie mit dem VSA darauf zugreifen können, selbst wenn die verwalteten Rechner abgeschaltet sind. Anhand von Inventarisierungen können Sie Konfigurationen überprüfen, bevor sich diese zu ernsthaften Problemen entwickeln. Das System führt drei Arten von Inventarisierungen für jede Rechner-ID durch:

- **Referenzinventarisierung** – Die Konfiguration des Systems in seinem Originalzustand. Normalerweise wird eine Referenzinventarisierung bei der Ersteinrichtung eines Systems durchgeführt.
- **Letzte Inventarisierung** – Die Konfiguration des Systems bei der letzten Inventarisierung. Empfohlen wird einmal pro Tag.
- **Systeminformationen** – Alle DMI/SMBIOS-Daten des Systems zum Zeitpunkt der letzten Systeminformationen-Inventarisierung. Diese Daten ändern sich praktisch nie, und dieser Vorgang muss normalerweise nur einmal ausgeführt werden.

Der VSA stellt Änderungen an der Rechnerkonfiguration fest, indem er das letzte Audit mit dem Basis-Audit vergleicht. Der Datensatz der letzten Inventarisierung wird für die angegebene Anzahl von Tagen gespeichert.

Der Großteil der Daten über Agents und verwalteten Rechnern auf den Funktionsseiten und unter "Infocenter > **Berichterstellung** *(siehe 164)* > Berichte" basieren auf dem letzten Audit. Der Bericht **Rechneränderungen** stellt einen Vergleich der letzten Inventarisierung und der Referenzinventarisierung einer Rechner-ID dar. Über zwei **Alarm** *(siehe 284)*typen wird spezifisch auf die Änderungen zwischen einer Referenzinventarisierung und der letzten Inventarisierung hingewiesen: **Anwendungsänderungen** und **Hardware-Änderungen**.

Aufgabentypen

Aufgabentypen bestimmen, wie Zeiteinträge mit anderen Funktionen in den VSA integriert werden. Die in Ihrem VSA angezeigten Aufgabentypoptionen hängen von den installierten Modulen ab.

- **Admin-Aufgaben** – Sich wiederholende, keinem Projekt zugeordnete Aktivitäten.
- **Arbeitsaufträge** – Werden nur bei Installation von **Service Billing** angezeigt.
- **Service-Desk-Tickets** – Werden nur bei Installation von **Service Desk** 1.3 oder später angezeigt.

Auto-Lernen – Monitor-Sets

Sie können **Auto-Lernen**-Alarmschwellenwerte für jedes Standard-Monitor-Set aktivieren, das Sie ausgewählten Rechner-IDs zuweisen. Damit werden Alarmschwellenwerte basierend auf tatsächlichen Leistungsdaten auf die einzelnen Rechner abgestimmt.

Jeder zugewiesene Rechner generiert Leistungsdaten für die angegebene Zeitspanne. Während dieser Zeitspanne werden keine Alarme ausgelöst. Am Ende der Auto-Lernen-Sitzung wird der Alarmschwellenwert für jeden zugewiesenen Rechner basierend auf der tatsächlichen Leistung des Rechners automatisch abgestimmt. Sie können die Alarmschwellenwerte, die durch **Auto-Lernen** berechnet wurden, manuell anpassen oder eine weitere **Auto-Lernen**-Sitzung ausführen. **Auto-Lernen** kann nicht mit individualisierten Monitor-Sets verwendet werden.

Automatische Installation

Bei automatischen Installationen, die auch als **automatische Bereitstellungen** bezeichnet werden, wird der Benutzer nicht zu Eingaben aufgefordert. Automatische Installationen erfordern entweder keine Benutzereingaben oder geben eine typische Konfiguration vor, die den Anforderungen der meisten Benutzer gerecht wird. Sie können auch Befehlszeilenparameter zur Verfügung stellen, anhand derer die Benutzer die Installation zum Zeitpunkt der Ausführung konfigurieren können. Falls eine Installation keine automatische Installation unterstützt, jedoch trotzdem automatisch verteilt werden muss, können Benutzer mit einem **Packager** *(siehe 623)* ein benutzerdefiniertes Installationspaket erstellen. Siehe **Automatische Installationen erstellen** *(siehe 132)*.

Automatisches Windows Update

Automatische Windows-Aktualisierung ist ein Microsoft-Tool, mit dem automatisch Aktualisierungen auf einem Computer bereitgestellt werden. Automatische Windows-Aktualisierung wird für die folgenden Betriebssysteme unterstützt: Windows 2003, Windows XP, Windows 2000 SP3 oder höher sowie alle nach diesen herausgegebenen Betriebssysteme. Über Patch-Management > Automatisches Windows Update kann diese Funktion auf verwalteten Rechnern aktiviert oder deaktiviert werden. Windows Millennium Edition (Me) unterstützt zwar Automatische Aktualisierungen, es kann jedoch nicht wie die obigen Betriebssysteme verwaltet werden.

Backup-Sätze

Alle für eine vollständige Sicherung benötigten Dateien, einschließlich aller inkrementellen oder differentiellen Sicherungen, werden zusammen in einem **Sicherungssatz** gespeichert.

Benutzer

VSA-Benutzer verwenden die VSA-Anwendung zum Pflegen des Kaseya Server und zum Überwachen des Monitoring von **verwalteten Rechnern** *(siehe 632)* durch den Kaseya Server und seine **Agents** *(siehe 611)*. VSA-Benutzer werden über die Seite System > **Benutzer** *(siehe 409)* erstellt. Als Benutzer werden auch Rechnerbenutzer bezeichnet, die vom VSA verwaltete Computer verwenden. **Hauptbenutzer** *(siehe 620)* verfügen über spezielle Berechtigungen für den gesamten VSA.

Benutzerkonto

Siehe **Rechner-IDs vs. Agent** *(siehe 627)*

Chat

Online-**Chat** ist ein textbasiertes Instant-Messaging-System. Es kommt zusammen mit dem Kaseya Server und dient hauptsächlich zur Bereitstellung von sofortigem technischem Support. VSA-Benutzer können mit Rechnerbenutzern und/oder anderen VSA-Benutzern chatten, die gleichzeitig am selben Kaseya Server angemeldet sind. VSA-Benutzer können die Fähigkeit eines Rechnerbenutzers, eine Chat-Sitzung mit VSA-Benutzern einzuleiten, aktivieren oder deaktivieren. Da Kaseya-Chats über den Kaseya Server übermittelt werden, sind alle Chats durch das Kaseya 256-Bit-Protokoll mit Rolling-Code-Verschlüsselung geschützt.

Check-in: Voll vs. Schnell

Ein **vollständiger Check-in** findet statt, wenn ein Agent die Verarbeitung aller ausstehenden Aufgaben,

die ihm von Kaseya Server zugewiesen wurden, abschließt. Diese Aufgaben können die Verarbeitung eines Agent-Verfahrens, das Einsenden gecachter Protokolldaten oder die Aktualisierung der Agent-Konfigurationsdatei einschließen. Ein vollständiger Check-in findet auch dann statt, wenn 24 Stunden vergehen, ohne dass eine bestimmte Aufgabe einen Check-in benötigt. Ein **schneller Check-in** findet statt, wenn sich ein Konto nach dem konfigurierten Check-in-Intervall eincheckt und dadurch dem Kaseya Server zu verstehen gibt, dass der verwaltete Rechner weiterhin online ist. Hierfür ist kein Abschluss aller ausstehenden Aufgaben erforderlich. Für manche Funktionen wird ein vollständiger Check-in benötigt, bevor ein Agent mit der Verarbeitung einer neuen Aufgabe beginnen kann. Zum Beispiel System > **Benennungsrichtlinie** *(siehe 406)*. Sie können einen vollständigen Check-in erzwingen, indem Sie mit der rechten Maustaste auf das Agent-Symbol in der Systemablage eines verwalteten Rechners klicken und dann auf die Option **Aktualisieren** klicken.

Dashboard

Im Dashboard wird eine Übersicht über den Status des gesamten Systems angezeigt. Die Dashboard-Daten werden nach **Rechner-ID/Gruppen-ID-Filter** *(siehe 626)* gefiltert. Navigation: Info Center > **Dashboard anzeigen** *(siehe 241)*.

Dashboardliste

Bei der Dashboardliste handelt es sich um eine Übersicht über die Alarmstatus aller überwachten Rechner. Die Dashboardlisten-Daten werden nach **Rechner-ID/Gruppen-ID-Filter** *(siehe 626)* gefiltert. Navigation: Info Center > **Dashboardliste** *(siehe 251)* oder Monitor > Dashboardliste.

Datei verteilen

Mit der Funktion **Datei verteilen** werden auf Ihrem VSA-Server gespeicherte Dateien an verwaltete Rechner übertragen. Sie eignet sich besonders für die Massenverteilung von Konfigurationsdateien (z. B. Virus-Footprints) oder für die Pflege der neuesten Version ausführbarer Dateien auf allen Rechnern. Der VSA prüft die Integrität der Datei bei jedem **vollständigen Check-in** *(siehe 616)*. Sollte die Datei jemals gelöscht oder beschädigt werden oder eine aktualisierte Version davon auf dem VSA verfügbar sein, überträgt der VSA vor jeder Verfahrensausführung eine neue Kopie. Verwenden Sie diese Funktion in Verbindung mit periodischen Verfahren, um Stapelbefehle auf verwalteten Rechnern auszuführen.

Dateiübertragungsprotokoll (File Transfer Protocol, FTP)

File Transfer Protocol (FTP) ist ein häufig verwendetes Protokoll für den Austausch von Dateien über jedes beliebige Netzwerk, dass das TCP/IP-Protokoll unterstützt. Der **FTP-Server** ist das Programm auf der Zielmaschine, das im Netzwerk auf Verbindungsanfragen von anderen Computern achtet. Der **FTP-Client** ist das Programm auf dem lokalen Rechner des VSA-Benutzers, das eine Verbindung zum Server initiiert. Der FTP-Clientrechner erfordert Benutzerzugriffsrechte für den FTP-Serverrechner. Es ist im Lieferumfang des Kaseya Server enthalten und dient hauptsächlich zur Bereitstellung von sofortigem technischem Support. Nach der Verbindung kann der Client Dateien auf den Server hochladen, Dateien vom Server herunterladen, Dateien auf dem Server umbenennen oder löschen usw. Jedes Softwareunternehmen oder jeder einzelne Programmierer kann FTP-Server- oder Clientsoftware erstellen, da das Protokoll ein offener Standard ist. Das FTP-Protokoll wird von praktisch jeder Computerplattform unterstützt. Da Kaseya-FTP-Sitzungen über den Kaseya Server übermittelt werden, sind alle FTP-Sitzungen durch das Kaseya-256-Bit-Protokoll mit Rolling-Code-Verschlüsselung geschützt.

Desktop aufzeichnen

Gilt nur für WinVNC. Wenn diese Option aktiviert ist, wird ein Video des Desktops aufgezeichnet und die aufgezeichnete Desktopsitzung bleibt im Arbeitsverzeichnis des Agent-Rechners gespeichert. Normalerweise kann ein Benutzer anhand einer Videoaufnahme einer Desktopsitzung sehen, welche Vorgänge ein Administrator während der Aufzeichnung an seinem Rechner durchgeführt hat. Dies schützt den Administrator vor Anschuldigungen, nicht autorisierte Änderungen am Rechner vorgenommen zu haben. Die Videos von Desktopsitzungen sind vom Arbeitsverzeichnis des Remote-Rechners aus zugänglich. Gilt nur für Rechner mit dem Windows- und Apple-Betriebssystem. Sitzungen mit der Aktivität **Desktop aufzeichnen** können an den folgenden Punkten gestartet und gestoppt werden:

- **Aufzeichnen von jeder Remote-Control-Sitzung** – Im Modul **Remote Control** kann das Kontrollkästchen **Remote Control in einer Datei im Arbeitsverzeichnis des Computers aufzeichnen** auf den Seiten **Benutzerrollen-Richtlinie** *(siehe 382)* und **Rechnerrichtlinie** *(siehe 383)* aktiviert werden. Jede Remote-Control-Sitzung, die auf diesen Richtlinien basiert, wird automatisch aufgezeichnet.
- **Aufzeichnen einer Remote-Control-Sitzung** – Auf der Seite **Rechnersteuerung** *(siehe 374)* kann vor dem Starten einer einzelnen Remote-Control-Sitzung auf einem Rechner das Kontrollkästchen **Remote Control in einer Datei im Arbeitsverzeichnis des Computers aufzeichnen** aktiviert werden.
- **Aufzeichnen ohne Remote-Control-Sitzung** – Mit der Schaltfläche **Desktop aufzeichnen** in der **Schnellanzeige** *(siehe 17)* wird der Desktop aufgezeichnet, ohne dass eine Remote-Control-Sitzung gestartet wird.

Einstellungen und Vorlagen kopieren

Rechner-ID-Vorlagen *(siehe 627)* werden anfänglich dazu verwendet, um ein Agent-Installationspaket zu erstellen. Dabei wird die Vorlage als Quelle verwendet, um Einstellungen zu kopieren. Aber selbst nach der Installation der Agents auf verwalteten Rechnern müssen Sie die Einstellungen auf vorhandenen Rechner-ID-Konten aktualisieren, da sich die Anforderungen Ihrer Kunden ändern und Sie sich immer besser mit dem VSA auskennen. Verwenden Sie in diesem Fall Agent > **Einstellungen kopieren**, um diese Änderungen auf alle Rechner-IDs zu kopieren, für die Sie Zugriffsberechtigungen haben. Achten Sie darauf, `Do Not Copy` für jede Einstellung auszuwählen, die Sie nicht überschreiben möchten. Verwenden Sie `Add`, um Einstellungen zu kopieren, ohne vorhandene Einstellungen zu entfernen. Kaseya empfiehlt, zuerst die Änderungen an einer ausgewählten Vorlage vorzunehmen und diese Vorlage dann als Quellrechner-ID zum Kopieren zu verwenden. Auf diese Weise wird sichergestellt, dass Ihre Rechner-ID-Vorlagen die "Master-Repositories" aller Ihrer Agent-Einstellungen bleiben und als Quelle für die Agent-Installationspakete und vorhandenen Rechner-ID-Konten dienen können.

Ereignisprotokolle

Ein **Ereignisprotokolldienst** wird auf Windows-Betriebssystemen ausgeführt. (Er steht nicht für Win9x zur Verfügung.) Über den Ereignisprotokolldienst können Ereignisprotokollnachrichten von Windows-basierten Programmen und Komponenten ausgegeben werden. Diese Ereignisse werden in den auf jedem Rechner gespeicherten Ereignisprotokollen gespeichert. Die Ereignisprotokolle verwalteter Rechner können in der Kaseya Server-Datenbank gespeichert werden und als Basis aller Meldungen und Berichte dienen. Sie können auch archiviert werden.

Abhängig vom jeweiligen Betriebssystem stehen die folgenden **Ereignisprotokolltypen** zur Verfügung:

- Anwendungsprotokoll
- Sicherheitsprotokoll
- Systemprotokoll
- Verzeichnisdienstprotokoll
- Dateireplikationsdienstprotokoll
- DNS-Serverprotokoll

Windows-Ereignisse werden über die folgenden **Ereignisprotokollkategorien** weiter klassifiziert:

- Fehler
- WARNUNG
- Informationen
- Erfolgs-Audit
- Fehler-Audit
- Kritisch – betrifft nur Vista, Windows 7 und Windows Server 2008
- Ausführlich – betrifft nur Vista, Windows 7 und Windows Server 2008

Ereignisprotokolle werden von den folgenden VSA-Seiten verwendet bzw. referenziert:

- Monitor > **Agent-Protokolle** *(siehe 35)*
- Monitor > **Ereignisprotokoll-Meldungen** *(siehe 316)*
- Monitor > Ereignisprotokoll-Meldungen > **Ereignissätze bearbeiten** *(siehe 320)*

- Monitor > **Listen nach Scan aktualisieren** *(siehe 266)*
- Agent > **Protokollverlauf** *(siehe 36)*
- Agent > **Ereignisprotokolleinstellungen** *(siehe 38)*
- Agent > **Agent-Protokolle** *(siehe 35)*
- Berichte > **Protokolle** *(siehe 625)*
- **Live-Connect** *(siehe 393)* > Ereignisanzeige
- **Schnellanzeige** *(siehe 17)* > Ereignisanzeige
- System > Datenbanksichten > **vNtEventLog** *(siehe 510)*

Ereignissätze

Da die Anzahl der Ereignisse in Windows-**Ereignisprotokollen** *(siehe 618)* riesig ist, verwendet der VSA einen Datensatztyp namens **Ereignissatz**, um nach Meldungsbedingungen zu filtern. Ereignissätze enthalten eine oder mehrere **Bedingungen**. Jede Bedingung enthält Filter für verschiedene Felder in einem **Ereignisprotokolleintrag**. Die Feld sind **Quelle**, **Kategorie**, **Ereignis-ID**, **Benutzer** und **Beschreibung**. Ein **Ereignisprotokoll** *(siehe 618)*eintrag muss alle Feldfilter einer Bedingung erfüllen, um als Übereinstimmung zu gelten. Ein Feld mit einem Sternchen (*) bedeutet, dass jede Zeichenfolge, selbst eine leere Zeichenfolge, als Übereinstimmung gilt. Eine Übereinstimmung auch nur *einer* der Bedingungen in einem Ereignissatz ist ausreichend, um eine Meldung für einen Rechner auszulösen, auf den dieser Ereignissatz angewendet wurde. Weitere Hinweise zum Konfigurieren von Ereignissätzen finden Sie unter Monitor > Ereignisprotokoll-Meldungen > **Ereignissätze bearbeiten** *(siehe 320)*.

Featuregruppe

Eine Featuregruppe stellt erweiterte, spezialisierte Funktionen bereit, die typischerweise im grundlegenden Modul abgeblendet sind. Das grundlegende Modul muss installiert sein und das Feature muss separat lizenziert werden, damit die Optionen für die Featuregruppe angezeigt werden.

Fluterkennung

Wenn 1000 Ereignisse (ohne Zählung der **Blacklist-Ereignisse** *(siehe 619)*) von einem Agent *innerhalb einer Stunde* auf den Kaseya Server hochgeladen werden, wird die weitere Erfassung von Ereignissen dieses Protokolltyps für den Rest der Stunde angehalten. Ein neues Ereignis wird in das Ereignisprotokoll eingefügt, um die Aussetzung der Erfassung zu verzeichnen. An Ende der Stunde wird die Erfassung automatisch wieder aufgenommen. Dies verhindert, dass der Kaseya Server von kurzfristigen Schwerlasten überschwemmt wird. Die Alarmermittlung und -verarbeitung wird ungeachtet einer ausgesetzten Erfassung fortgesetzt.

Globale Ereignisprotokolllisten

Jeder Agent verarbeitet zwar alle Ereignisse, die auf einer "Blacklist" aufgeführten Ereignisse werden jedoch *nicht* auf den VSA-Server hochgeladen. Es gibt zwei "Blacklists". Eine wird periodisch von Kaseya aktualisiert und trägt die Bezeichnung `EvLogBlkList.xml.`. Die zweite mit dem Namen `EvLogBlkListEx.xml` kann vom Dienstanbieter verwaltet werden und wird nicht von Kaseya aktualisiert. Beide befinden sich im Verzeichnis `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles`. Die Alarmermittlung und -verarbeitung werden fortgesetzt, ungeachtet dessen, ob sich die Einträge in der Erfassungs-Blacklist befinden oder nicht.

Gruppenalarme

Alarme für Meldungen, Ereignisprotokoll-Meldungen, Systemprüfung und Protokoll-Monitoring werden automatisch einer **Gruppenalarm**-Kategorie zugewiesen. Beim Auslösen eines Alarms wird auch der zugehörige Gruppenalarm ausgelöst. Die Gruppenalarm-Kategorien für Monitor-Sets und SNMP-Sets werden bei der Definition der Sets manuell zugewiesen. Gruppenalarme werden im Dashlet **Gruppenalarmstatus** *(siehe 256)* der Seite Monitor > **Dashboard-Liste** angezeigt. Sie können neue Gruppen über die Registerkarte **Gruppenalarm-Spaltennamen** in Monitor > **Monitorlisten** *(siehe 264)* erstellen. Gruppenalarmspalten werden Monitor-Sets über **Monitor-Set definieren** *(siehe 269)* zugewiesen.

Hostname

Dies ist das Textäquivalent einer IP-Adresse. Zum Beispiel sollte die IP-Adresse `89.234.7.197` in den Hostnamen `www.kaseya.com` aufgelöst werden.

ISO-Abbild

Ein **ISO-Abbild (.iso)** ist ein Plattenabbild eines ISO 9660-Dateisystems. ISO 9660 ist ein internationaler Standard, der ursprünglich für die Speicherung von Daten auf CD-ROM entwickelt wurde. Neben den Datendateien, die in dem ISO-Abbild enthalten sind, beinhaltet das ISO-Abbild auch sämtliche Metadaten des Dateisystems, einschließlich *Bootcode*, Strukturen und Attribute. Alle diese Informationen sind in einer einzigen Datei enthalten. CD-Writer stellen beim Schreiben auf CD für gewöhnlich die Option zum Schreiben einer ISO-Datei *als ein Abbild* zur Verfügung.

Kanonischer Name

Der primäre Name eines Objekts in DNS. Jedes Objekt kann darüber hinaus eine unbegrenzte Anzahl von Aliasen besitzen.

LAN-Watch

LAN-Watch im **Discovery**-Modul verwendet einen bestehenden VSA-**Agent** *(siehe 611)* auf einem verwalteten Rechner, um das lokale Netzwerk auf beliebige und alle neuen Geräte zu scannen, die seit der letzten Ausführung von LAN-Watch an dieses LAN angeschlossen wurden. Diese neuen Geräte können Workstations und Server ohne Agents, **SNMP-Geräte** *(siehe 629)* und vPro-Rechner sein. Der VSA kann optional eine **Meldung** *(siehe 621)* senden, wenn LAN-Watch ein neues Gerät ermittelt. LAN-Watch verwendet den Agent im Grunde genommen als Proxy, um ein LAN hinter einer Firewall zu scannen, auf das nicht von einem Remote Server aus zugegriffen werden kann.

Leistungsobjekte, Instanzen und Zähler

Beim Einrichten von Zählerschwellenwerten in **Monitor-Sets** *(siehe 622)* ist zu beachten, wie Windows und der VSA die zu überwachenden Komponenten identifizieren:

- **Leistungsobjekt** – Eine logische Sammlung von Zählern, die mit einer Ressource oder einen Dienst verknüpft sind, der überwacht werden kann. Zum Beispiel: Prozesse, Arbeitsspeicher, physikalische Festplatten und Server haben alle ihre eigenen Sätze vordefinierter Zähler.
- **Leistungsobjekt-Instanz** – Ein Begriff, mit dem zwischen mehreren Leistungsobjekten des gleichen Typs auf einem Computer unterschieden wird. Zum Beispiel: mehrere Prozessoren oder mehrere physikalische Festplatten. Der VSA lässt Sie dieses Feld überspringen, falls nur eine Instanz eines Objekts vorliegt.
- **Leistungszähler** – Ein mit einem Leistungsobjekt und gegebenenfalls mit der Instanz verknüpftes Datenelement. Jeder ausgewählte Zähler stellt einen Wert das, der einem bestimmen Aspekt der Leistung entspricht, die für das Leistungsobjekt und die Instanz definiert wurden.

Lokal

Eine **lokale** Hardware-/Softwareinstallation des VSA wird von einem Dienstanbieter gepflegt und in der Regel nur von diesem Dienstanbieter eingesetzt. Siehe **Software as a Service (SaaS)** *(siehe 631)*.

MAC-Adresse

Der eindeutige Identifikator **Media Access Control (MAC)**, der Netzwerkkarten (NICs) zugewiesen wird

Master-Benutzer/Standardbenutzer

Ein Master-Benutzer ist ein VSA-**Benutzer** *(siehe 616)* mit `Master`-Benutzerrolle und `Master`-Scope. Die `Master`-Benutzerrolle bietet Benutzerzugriff auf alle Funktionen im gesamten VSA. Der `Master`-Scope stellt Zugriff auf alle Scope-Datenobjekte im gesamten VSA bereit. Eine `Master`-Benutzerrolle kann zwar mit einem Nicht-`Master`-Scope verwendet werden, ein `Master`-Scope aber nicht mit einer Nicht-`Master`-Rolle. Die Kaseya Server-Verwaltungskonfiguration und andere **spezialisierte Funktionen** *(siehe 414)* können nur von Benutzern mit `Master`-Rolle ausgeführt werden. Der Begriff *Standardbenutzer* wird manchmal für einen Benutzer ohne `Master`-Rolle und `Master`-Scope

verwendet.

Meldung

Meldungen sind Antworten auf **Meldungsbedingungen** *(siehe 621)*. Sie unterscheiden sich von einer **Inventarisierung** *(siehe 615)*, bei der ohne Berücksichtigung irgendwelcher Kriterien lediglich ausgewählte Daten zu Referenzzwecken gesammelt werden.

Es gibt zwei Arten von Meldungen, generische und spezifische:

Generische Meldungen

Es gibt in der Regel vier Arten von Antworten auf eine Meldungsbedingung:

- **A**larm erstellen
- **T**icket erstellen
- Verfahren ausführen
- **E**-Mail-Empfänger

Durch die Definition einer Meldung wird der **ATSE-Antwortcode** *(siehe 621)* für diese Rechner-ID oder dieses SNMP-Gerät festgelegt.

Meldungen werden folgendermaßen definiert:

- Monitor > **Meldungen** *(siehe 284)*
- Monitor > **Monitor zuweisen** *(siehe 327)*
- Monitor > **SNMP zuweisen** *(siehe 340)*
- Monitor > **Systemprüfungen** *(siehe 336)*
- Monitor > **Analyse-Übersicht** *(siehe 353)*
- Monitor > **Analysesätze zuweisen** *(siehe 363)*
- Patch-Management > Patch-Meldungen
- Fernsteuerung > Externe Meldungen
- Sicherung > Sicherungsmeldungen
- Sicherheit > Alarmsätze anwenden
- Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*

Spezifische Meldungen

Über die Seite **Meldungen** können Sie im Handumdrehen Meldungen für typische **Meldungsbedingungen** *(siehe 621)* definieren, die in einer IT-Umgebung vorgefunden werden. So ist beispielsweise geringer Plattenspeicherplatz ein häufiges Problem bei verwalteten Rechnern. Bei Auswahl des Meldungstyps `Low Disk` wird ein einzelnes zusätzliches Feld angezeigt, in dem Sie den `% free space`-Schwellenwert definieren können. Anschließend können Sie diese Meldung unmittelbar auf jede auf der Seite **Meldungen** angezeigte Rechner-ID anwenden und die Reaktion auf die Meldung festlegen.

Meldungen

Eine Meldung wird erstellt, wenn die Leistung eines Rechners oder Geräts mit einem vordefinierten Kriterium oder einer „Meldungsbedingung“ übereinstimmt.

Meldungsaktionen

Erstellen eines Alarms ist nur ein *Aktionstyp*, der ergriffen werden kann, wenn eine Meldung auftritt. Die anderen Aktionstypen sind Benachrichtigungen. Diese umfassen **das Senden einer E-Mail** oder **Erstellen eines Tickets**. Ein vierter Aktionstyp ist das **Ausführen eines Agent-Verfahrens**, um automatisch auf die Meldung zu reagieren. Diese vier Arten von Aktionen werden als **ATSE-Code** bezeichnet. Der ATSE-Code gibt an, welche Arten von Aktionen für die definierte Meldung aktiv sind, unabhängig davon, ob sie einer Rechner-ID, einer Gruppen-ID oder einem SNMP-Gerät zugewiesen sind.

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen

- E = **E**-Mail-Empfänger

Keine der ATSE-Aktionen wird benötigt. Die Meldung und die ATSE-Aktion (einschließlich keine Aktion) werden im Bericht Info Center > Monitor – **Monitor-Aktionsprotokoll** *(siehe 224)* ausgegeben.

Meldungstypen

Meldungen sind einer der verschiedenen **Monitortypen** *(siehe 623)* auf.
1 – Adminkonto deaktiviert
2 – Meldung 'Dateiänderung abrufen'
3 – Neuer Agent hat das erste Mal eingecheckt
4 – Anwendung installiert oder gelöscht
5 – Agent-Verfahrensfehler festgestellt
6 – Fehler in NT-Ereignisprotokoll festgestellt
7 – Kaseya Server beendet
8 – Schutzverletzung festgestellt
9 – PCI-Konfiguration geändert
10 – Festplattenlaufwerkskonfiguration geändert
11 – RAM-Größe geändert
12 – Test-E-Mail von serverInfo.asp gesendet
13 – Geplanter Bericht abgeschlossen
14 – LAN-Watch-Meldungstyp
15 – Agent offline
16 – Festplattenspeicher niedrig
17 – Remote Control deaktiviert
18 – Agent online
19 – Neues Patch gefunden
20 – Patch-Pfad fehlt
21 – Patch-Installation fehlgeschlagen
23 – Backup-Meldung

Meldungstypen

Zu den Arten von Meldungen gehören:

- Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*
- Sicherung > Sicherungsmeldungen
- Monitor > **Meldungen** *(siehe 284)* – Dies sind spezielle „festgelegte“ Meldungen, die sofort auf einen Rechner angewendet werden können.
- Monitor > **Monitor zuweisen** *(siehe 327)*
- Monitor > **SNMP-Traps-Meldung** *(siehe 323)*
- Monitor > **SNMP zuweisen** *(siehe 340)*
- Monitor > **Systemprüfungen** *(siehe 336)*
- Monitor > **Analyse-Übersicht** *(siehe 353)*
- Monitor > **Analysesätze zuweisen** *(siehe 363)*
- Patch-Management > Patch-Meldungen
- Fernsteuerung > Externe Meldungen
- Sicherheit > Alarmsätze anwenden

Andere Zusatzmodule verfügen über Meldungen, die hier nicht aufgelistet sind.

Migrieren des Kaseya Server

Die neuesten Anweisungen zur Migration eines vorhandenen Kaseya Server auf einen neuen Rechner finden Sie im Abschnitt *Verschieben des Kaseya Server* in den aktuellen **Kaseya Server-Installationsanweisungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/Install/index.asp#home.htm)*.

Monitor-Sets

Ein Monitor-Set ist ein Satz von **Zählerobjekten**, **Zählern**, **Zählerinstanzen**, **Diensten** und **Prozessen**, anhand

derer die Leistung von Rechnern überwacht werden kann. In der Regel wird jedem/jeder **Objekt/Instanz/Zähler** *(siehe 620)*, Dienst oder Prozess in einem Monitor-Set ein Schwellenwert zugewiesen. Sie können Alarme festlegen, die ausgelöst werden, wenn einer der Schwellenwerte im Monitor-Set überschritten wird. Ein Monitor-Set sollte als eine logische Gruppierung von Faktoren, die überwacht werden sollen, verstanden werden. Eine solche logische Gruppierung könnte beispielsweise die Überwachung alle zum Ausführen eines Exchange Server erforderlichen Zähler und Dienste sein. Sie können jedem Rechner, auf dem das Betriebssystem Windows 2000 oder höher ausgeführt wird, ein Monitor-Set zuweisen.

Das allgemeine Verfahren zum Arbeiten mit Monitor-Sets ist wie folgt:

1. Sie können die Objekte, Instanzen und Zähler von Monitor-Sets über **Monitorlisten** *(siehe 264)* wahlweise auch manuell aktualisieren und prüfen.
2. Erstellen und pflegen Sie Monitor-Sets über Monitor > **Monitor-Sets** *(siehe 267)*.
3. Weisen Sie Monitor-Sets über Monitor > **Monitor zuweisen** *(siehe 327)* bestimmten Rechner-IDs zu.
4. Wahlweise können Sie Standard-Monitor-Sets als *individualisierte Monitor-Sets* anpassen.
5. Die wahlweise Anpassung von Standard-Monitor-Sets erfolgt über *Auto-Lernen*.
6. Überprüfen Sie Monitor-Sets über folgende Befehle:
   - Monitor > **Monitor-Protokoll** *(siehe 333)*
   - Monitor > **Live Counter** *(siehe 263)*
   - Monitor > Dashboard > **Netzwerkstatus** *(siehe 255)*
   - Monitor > Dashboard > **Gruppenalarmstatus** *(siehe 256)*
   - Monitor > Dashboard > **Monitor-Set-Status** *(siehe 256)*
   - Info Center > Reporting > Berichte > Monitor > Monitor-Set-Bericht
   - Info Center > Reporting > Berichte > Monitor > Monitor-Aktionsprotokoll

Monitortypen

0 - Zähler
1 - Dienst
2 - Prozess
3 - SNMP
4 - Alarm - Alarme werden weiter nach ihren **Alarmtypen** *(siehe 622)* unterteilt.
5 - Systemprüfung
6 - EPS
7 - Protokollkontrolle

myOrg

`myOrg` ist die **Organisation** *(siehe 623)* des Dienstanbieters, der den VSA verwendet. Alle anderen Organisationen im VSA sind Fremdorganisationen, die mit `myOrg` geschäftliche Beziehungen unterhalten. Der Standardname `myOrg`, `My Organization`, sollte in den Firmennamen des Dienstanbieters umbenannt werden. *Dieser Name wird oben auf verschiedenen Berichten angezeigt, um dem Bericht ein Branding zu verleihen.* Agents, die auf intern verwalteten Rechnern installiert sind, können dieser Organisation zugewiesen werden. *VSA-Benutzeranmeldedaten sind üblicherweise mit Mitarbeiterdatensätzen in der Organisation* `myOrg` *verknüpft.* `myOrg` kann keiner übergeordneten Organisation zugeordnet werden.

Objekt-Manager

Der **Packager** ist ein Assistent zum Erstellen eines Pakets, wenn keine vordefinierte Installationslösung verwendet werden kann. Der **Packager** wertet den Zustand eines Quellrechners vor und nach einer Installation und/oder Änderung der Ressource aus. Der **Packager** übersetzt die Abweichungen in eine einzelne, ausführbare Datei (das **Paket**), die dann über Agent-Verfahren auf jeden verwalteten Rechner verteilt werden kann. Verteilen Sie ein Paket auf beliebige Weise. Sie können es per E-Mail senden oder auf einem Server speichern, wo ein **benutzerdefiniertes Verfahren** *(siehe 92)* eine automatische Installation auf jedem verwalteten Rechner ausführen kann.

Org

Der VSA unterstützt drei verschiedene Arten von Geschäftsbeziehungen:

- **Unternehmen** – Unterstützung von Rechnergruppen und Verwaltung von Rechnern mittels Agents.
- **Kunden** – Unterstützung der Fakturierung von Kunden mittels **Service Billing**.
- **Anbieter** – Unterstützung der Materialbeschaffung mittels **Service Billing**.

Die `Org`-Tabelle ist eine Supporttabelle, die von *Unternehmen*, *Kunden* und *Anbietern* gemeinsam genutzt wird. Jeder Datensatz in der `Org`-Tabelle wird durch eine eindeutige `orgID` identifiziert. Die `Org`-Tabelle enthält grundlegende Informationen, die Sie generell zur Pflege von Geschäftsbeziehung aller Art benötigen: Postanschrift, primäre Telefonnummer, DUNS-Nummer, Jahreseinnahmen usw. Da die `Org`-Tabelle gemeinsam genutzt wird, können Sie folgende Umwandlungen mühelos vornehmen:

- Einen Kunden in ein Unternehmen oder einen Anbieter
- Einen Anbieter in ein Unternehmen oder einen Kunden
- Ein Unternehmen in einen Kunden oder Anbieter

Hinweis: `myOrg` (siehe 623) ist die Organisation des Dienstanbieters, der den VSA verwendet.

Patch-Richtlinie

Patch-Richtlinien enthalten alle aktiven Patches zum Zweck des Bestätigens oder Ablehnens von Patches. Ein aktives Patch ist als ein Patch definiert, das durch einen Patch-Scan von mindestens einem Rechner im VSA gemeldet wurde. Ein Rechner kann als Mitglied einer oder mehrerer Patch-Richtlinie(n) festgelegt werden.

Sie können beispielsweise eine Patch-Richtlinie namens `servers` erstellen und alle Ihre Server als Mitglieder dieser Patch-Richtlinie zuweisen. Dann erstellen Sie eine weitere Patch-Richtlinie namens `workstations` und weisen alle Ihre Workstations als Mitglieder dieser Richtlinie zu. Auf diese Weise können Sie unterschiedliche Patch-Bestätigungen für Server und Workstations konfigurieren.

- Die Patches von Rechnern, die keine Mitglieder irgendeiner Patch-Richtlinie sind, werden als *automatisch bestätigt* angesehen.
- Beim Erstellen einer neuen Patch-Richtlinie wird ihr Standard-Bestätigungsstatus für alle Patch-Kategorien auf *Bestätigung ausstehend* gesetzt.
- Der Standard-Bestätigungsstatus für jede Kategorie von Patches und für jedes Produkt kann separat festgelegt werden.
- Falls ein Rechner ein Mitglied mehrerer Patch-Richtlinien ist und diese Richtlinien miteinander in Konflikt stehende Bestätigungsstatus aufweisen, so gilt der am meisten einschränkende Bestätigungsstatus.
- Für die Eingangsaktualisierung und Automatische Aktualisierung müssen Patches bestätigt werden, bevor sie installiert werden.
- Mit Bestätigung nach Richtlinie wird ein Patch nach *Richtlinie* bestätigt oder abgelehnt.
- Mit Bestätigung nach Patch werden Patches nach *Patch* bestätigt oder abgelehnt und der Bestätigungsstatus für dieses Patch in allen Patch-Richtlinien festgelegt.
- Mit KB überschreiben wird der Standard-Bestätigungsstatus nach *KB-Artikel* für alle Patch-Richtlinien überschrieben und der Bestätigungsstatus für diejenigen Patches, auf die sich der KB-Artikel bezieht, in allen Patch-Richtlinien festgelegt.
- Mit Patch-Aktualisierung und Rechneraktualisierung können auch abgelehnte Patches installiert werden.
- Benutzer, die keine Haupt- bzw. `Master`-Rolle innehaben, sehen nur die von ihnen selbst erstellten Patch-Richtlinien bzw. Patch-Richtlinien mit Rechner-IDs, deren Umfang den Benutzer zur Anzeige autorisieren.

Planen als Agent-Zeit

Mit **Planen als Agent-Zeit** wird durch die vom Agent-Rechner verwendete Systemuhr der Zeitpunkt des

geplanten Vorgangs festgelegt. Durch die Planung des gleichen Vorgangs für zehn Rechner am Dienstag um 14 Uhr tritt dieser Vorgang auf jedem Rechner am Dienstag um 14 Uhr lokale Zeit – gemäß der Systemuhr jedes Rechners – auf. Über die Seite System > Serververwaltung > **Standardeinstellungen** *(siehe 437)* können Sie allgemein festlegen, ob entweder die Serverzeit oder Agent-Zeit standardgemäß zur Planung herangezogen werden soll.

Portalzugriff

Als Portalzugriff bezeichnet man eine von dem Rechnerbenutzer initiierte **Live Connect** *(siehe 393)*-Sitzung. Der Rechnerbenutzer zeigt die Seite **Portalzugriff** durch Klicken auf das Agent-Symbol auf der Systemablage eines verwalteten Rechners an. Auf der Seite **Portalzugriff** befinden sich Benutzeroptionen, beispielsweise zum Ändern der Kontaktinformationen des Benutzers, zum Erstellen oder Nachverfolgen von Tickets, zum Chatten mit VSA-Benutzern oder für die Fernsteuerung des eigenen Rechners von einem anderen Rechner aus. **Portalzugriff**-Anmeldungen werden über Agent > **Portalzugriff** *(siehe 75)* definiert. Die Funktionsliste, die dem Benutzer während einer **Portalzugriff**-Sitzung angezeigt wird, wird über die Seite System > **Rechnerrollen** *(siehe 417)* eingerichtet. Sie können **Portalzugriff**-Sitzungen über die Seite > Anpassen > **Live-Connect** *(siehe 452)* bedarfsgerecht gestalten. Die Installationsprogramme für die **Live-Connect**- und **Portalzugriff**-Plug-ins können über die Seite Agent > **Agent aktualisieren** *(siehe 81)* vorinstalliert werden.

Primärer Domain-Controller

Primäre Domain-Controller haben uneingeschränkten Zugriff auf die auf ihren Rechnern gespeicherten Kontodatenbanken. Nur primäre Domain-Controller können **Active Directory** *(siehe 611)* ausführen.

Private Ordner

Private Ordner

Von Ihnen erstellte Objekte, z. B. Berichte, Verfahren oder Monitorsets, werden anfänglich in einem Ordner mit Ihrem Benutzernamen unterhalb eines **Privat**-Cabinet gespeichert. Dies bedeutet, dass nur Sie, der Ersteller der Objekte in diesem Ordner, diese Objekte anzeigen, bearbeiten, ausführen, löschen oder umbennen können.

Um ein privates Objekt an andere Benutzer freizugeben, müssen Sie es zuerst in einen Ordner unterhalb des Cabinet **Gemeinsam nutzen** ziehen und dort ablegen.

> **Hinweis:** Ein Benutzer mit Master-Rolle kann das Kontrollkästchen **Freigegebene und private Ordnerinhalte aller Benutzer anzeigen** unter "System > **Voreinstellungen** *(siehe 402)*" aktivieren, um alle gemeinsam genutzten und privaten Ordner anzuzeigen. Dies gilt nur für private Ordner: Das Aktivieren dieses Kontrollkästchens verleiht dem Benutzer mit Master-Rolle genau wie dem Eigentümer sämtliche Zugriffsrechte.

Protokolle

In Protokollen werden Ereignisinformationen zu mehreren Systemen, einschließlich des Kaseya Server, gesammelt. Die folgenden Arten von Protokollen können generiert werden:

- **Administratoranmerkungen** – Hier werden Benutzeranmerkungen nach Benutzer sortiert aufgelistet.
- **Agent-Protokoll** – Dieses Protokoll zeigt eine Liste der mit dem Agent-Rechner verknüpften Aktivitäten an. Hier werden Start- und Stoppzeiten, Änderungen an der `.ini`-Datei und andere Informationen aufgezeichnet. Das Datum und die Uhrzeit jeder Aktivität werden ebenfalls vermerkt.
- **Agent-Verfahrensprotokoll** – Zeigt eine Liste der Verfahren an, die auf dem ausgewählten Agent-Rechner ausgeführt wurden. Das Datum und die Uhrzeit jedes Verfahrens werden ebenfalls vermerkt ebenso wie die Tatsache, ob es erfolgreich abgeschlossen wurde oder nicht.
- **Alarmprotokoll** – Listet alle ausgelösten Alarme auf, die für den ausgewählten Rechner ausgegeben wurden.

- **Konfigurationsänderungen** – Zeigt ein Protokoll der Änderungen an, die von einem Benutzer an der Agent-Konfiguration eines verwalteten Rechners vorgenommen wurden.
- **Ereignisprotokolle** – Zeigt die von Windows gesammelten **Ereignisprotokoll** *(siehe 618)*daten an. (Nicht mit Win9x verfügbar)
- **Protokoll-Monitoring** – Ermöglicht Ihnen, die von jedem textbasierten Protokoll generierten Daten zu überwachen.
- **Monitor-Aktionsprotokoll** – Das Protokoll der **Meldungsbedingungen** *(siehe 621)* sowie die entsprechenden Aktionen, die als Antwort darauf ergriffen wurden.
- **Netzwerkstatistiken** – Zeigt eine Liste der Anwendungen, die auf das Netzwerk zugegriffen haben, sowie die Paketgröße der Informationen, die während des Netzwerkzugriffs ausgetauscht wurden. Die Uhrzeit des Austauschs wird ebenfalls aufgeführt.
- **Fernsteuerungsprotokoll** – Listet die erfolgreichen Fernsteuerungsssitzungen auf.

Protokoll-Monitoring

Der VSA kann die aus zahlreichen **Standardprotokolldateien** *(siehe 625)* gesammelten Daten überwachen. **Protokoll-Monitoring** erweitert diese Fähigkeit noch weiter, indem Daten von der Ausgabe einer beliebigen textbasierten Protokolldatei extrahiert werden können. Beispiele hierfür sind Anwendungsprotokolldateien und **syslog** *(siehe 631)*-Dateien, die für Unix-, Linux- und Apple-Betriebssysteme und für Netzwerkgeräte wie etwa Cisco-Router erstellt wurden. Damit nicht alle in diesen Protokollen enthaltenen Daten in die Kaseya Server-Datenbank hochgeladen werden, verwendet die **Protokoll-Monitoring Analysedefinitionen und Analysesätze** *(siehe 613)* zum Analysieren jeder Protokolldatei und wählt nur diejenigen Daten aus, an denen Sie interessiert sind. Analysierte Nachrichten werden im Protokoll-Monitoring angezeigt, das Sie über die Registerkarte „Agent-Protokolle“ der Seite **Live Connect** *(siehe 393)* > Agent-Daten oder **Rechnerübersicht** *(siehe 151)* oder durch Generieren eines Berichts über die Seite Agent > Protokolle > **Protokoll-Monitoring** *(siehe 221)* aufrufen können. Benutzer können wahlweise beim Generieren eines **Protokoll-Monitoring**-Datensatzes Meldungen auslösen, laut Definition mit **Analysesätze zuweisen** *(siehe 363)* oder **Analyseübersicht** *(siehe 353)*.

Rechner-ID/Gruppen-ID/Organisation-ID

Jedem auf einem verwalteten Rechner installierten **Agent** *(siehe 611)* wird eine eindeutige **Rechner-ID/Gruppen-ID/Organisations-ID** zugewiesen. Alle Rechner-IDs gehören zu einer Rechnergruppen-ID und optional auch zu einer Untergruppen-ID. Alle Rechnergruppen-IDs gehören zu einer Organisations-ID. Eine Organisation stellt normalerweise ein einziges Kundenkonto dar. In einer kleinen Organisation ist vielleicht nur eine einzige Rechnergruppe vorhanden, die alle Rechner-IDs in dieser Organisation enthält. Eine große Organisation verfügt eventuell über viele Rechnergruppen und Untergruppen, die normalerweise nach Standort oder Netzwerk organisiert sind. Der vollständige Identifikator für einen auf einem verwalteten Rechner installierten Agent könnte beispielsweise als `jsmith.sales.chicago.acme` definiert werden. In diesem Fall stellt `sales` eine Untergruppen-ID innerhalb der Gruppen-ID `chicago` in der Organisations-ID namens `acme` dar. An manchen Stellen auf dem VSA wird diese Hierarchie im umgekehrter Reihenfolge angezeigt. Jede Organisations-ID hat eine einzige standardmäßige Rechnergruppen-ID namens `root`. Gruppen-IDs und Untergruppen-IDs werden über die Seite System > Orgs/Group/Depts/Staff > Verwalten > **Machine Groups** *(siehe 425)* erstellt.

Rechner-ID-/Gruppen-ID-Filter

Der Rechner-ID-/Rechnergruppen-ID-Filter steht auf allen Registerkarten und in allen Funktionen zur Verfügung. Mit seiner Hilfe können *Sie* anstelle eines Administrators die auf *allen* Funktionsseiten angezeigten Rechner beschränken. Über das Fenster **Definitionen anzeigen** können Sie einen Rechner-ID-/Rechnergruppen-Filter basierend auf den auf jedem Rechner enthaltenen Attributen (wie beispielsweise dem Betriebssystemtyp) weiter verfeinern. Nachdem Sie die Filterparameter angegeben haben, klicken Sie auf die Schaltfläche **Anwenden**, um die Filtereinstellungen auf *alle* Funktionsseiten anzuwenden. Der Rechner-ID-/Rechnergruppen-ID-Filter zeigt standardmäßig alle Rechner-IDs in `<All Groups>` an, die vom gegenwärtig angemeldeten VSA-Benutzer verwaltet werden.

> **Hinweis:** Selbst wenn ein VSA-Benutzer `<All Groups>` auswählt, werden nur Gruppen angezeigt, auf die dem VSA-Benutzer über System > Benutzersicherheit > **Scopes** *(siehe 419)* Zugriff gewährt wurde.

Rechner-IDs vs. Agents

Bei der Erläuterung von Agents ist es nützlich, zwischen der **Rechner-ID/Gruppen-ID/Organisations-ID** *(siehe 626)* und dem **Agent** *(siehe 611)* zu unterscheiden. Die Rechner-ID/Gruppen-ID/Organisations-ID ist der **Kontoname** für einen verwalteten Rechner in der VSA-Datenbank. Der Agent ist die Clientsoftware, die auf dem verwalteten Rechner installiert ist. Zwischen dem Agent auf einem verwalteten Rechner und seinem Kontonamen auf dem VSA besteht eine Eins-zu-Eins-Beziehung. Die Agent-Aktionen auf dem verwalteten Rechner werden von den Aufgaben geleitet, die einer Rechner-ID von VSA-Benutzern zugewiesen wurden.

Rechner-ID-Vorlage

Eine Rechner-ID-Vorlage ist ein *Rechner-ID-Datensatz ohne Agent*. Da sich ein Agent niemals an einem Rechner-ID-Vorlagenkonto anmeldet, wird er nicht in die Gesamtzahl Ihrer Lizenzen eingerechnet. Sie können kostenlos so viele Rechner-ID-Vorlagen erstellen, wie Sie wünschen. Beim Erstellen eines Agent-Installationspakets werden die Paketeinstellungen normalerweise von einer ausgewählten Rechner-ID-Vorlage kopiert. Für gewöhnlich werden Rechner-ID-Vorlagen für bestimmte Rechnertypen erstellt und konfiguriert. Rechnertypen umfassen Desktops, Autocad, QuickBooks, Small-Business-Server, Exchange-Server, SQL-Servers usw. **Basierend auf der von Ihnen definierten Rechner-ID-Vorlage kann ein entsprechendes Installationspaket erstellt werden.**

- Erstellen Sie Rechner-ID-Vorlagen über Agent > **Erstellen** *(siehe 55)*.
- Importieren Sie eine Rechner-ID-Vorlage über Agent **Import/Export** *(siehe 64)*.
- Erstellen Sie ein Agent-Installationspaket basierend auf einer Rechner-ID-Vorlage über Agent > **Agents bereitstellen** *(siehe 40)*.
- Kopieren Sie *ausgewählte* Einstellungen von Rechner-ID-Vorlagen auf vorhandene Rechner-ID-Konten über Agent > **Einstellungen kopieren** *(siehe 62)*.
- Bestimmen Sie die Gesamtzahl der Rechner-ID-Vorlagenkonten in Ihrem VSA über System > **Statistiken** *(siehe 442)*.
- Konfigurieren Sie Einstellungen für die Rechner-ID-Vorlage mithilfe der Standard-VSA-Funktionen, genau wie Sie ein Rechner-ID-Konto ohne Agent konfigurieren würden.
- Für Windows-, Apple- und Linux-Rechner werden separate Rechner-ID-Vorlagen empfohlen. Alternativ können Sie ein Paket erstellen, das das entsprechende Betriebssystem automatisch auswählt und Einstellungen von einer Vorlage kopiert, die ein Agent-Verfahren mit bestimmten Schritten das für das jeweilige Betriebssystemt enthält.

Rechnerrollen

Auf der Seite **Rechnerrollen** (siehe 414) werden Rechnerrollen erstellt und gelöscht. Rechnerrollen bestimmen, was *Rechnerbenutzern* bei der Verwendung des **Portalzugriffs** *(siehe 75)* – einer Version von **Live-Connect** *(siehe 393)* – auf einem Rechner mit Agent angezeigt wird. Das Fenster **Portalzugriff** wird angezeigt, wenn ein *Rechnerbenutzer auf das Agent-Symbol in der Systemablage seines verwalteten Rechners doppelklickt.*

> **Hinweis:** Die Seite **Benutzerrollen** bestimmt, was *VSA-Benutzern* bei der Verwendung von **Live-Connect** innerhalb des VSA angezeigt wird.

Auf der Seite **Rechnerrollen** können Sie Folgendes auswählen:

- **Mitglieder** *(siehe 418)* – Weisen Sie einer Rechnerrolle Rechner zu bzw. entfernen Sie sie.
- **Zugriffsrechte** *(siehe 418)* – Wählen Sie die Zugriffsrechte für die Rechnerrolle aus. Zugriffsrechte bestimmen die Funktionen, auf die ein *Rechnerbenutzer* Zugriff hat.

- **Rollentypen** *(siehe 419)* – Weisen Sie einer Rechnerrolle Rollentypen zu bzw. entfernen Sie sie. Gegenwärtig gibt es nur einen Rechnerrollentyp. Eine Beschränkung der Zugriffsrechte findet nicht statt.

Reihenfolge der Patch-Aktualisierung

Service Packs und Patches werden in der folgenden Reihenfolge installiert:

1. Windows-Installationsprogramm
2. Zum Betriebssystem gehörige Service Packs
3. Aktualisierungs-Rollups für das Betriebssystem
4. Kritische Aktualisierungen für das Betriebssystem
5. Nicht-kritische Aktualisierungen für das Betriebssystem
6. Sicherheitsaktualisierungen für das Betriebssystem
7. Service Packs für Office
8. Aktualisierungs-Rollups für Office
9. Alle übrigen Office-Aktualisierungen

> **Hinweis:** Neustarts werden nach jeder Installation eines Service Packs und am Ende jeder Patch-Gruppe **ohne Vorwarnung** erzwungen. Dies ist notwendig, damit ein erneuter Scan stattfinden kann und die Installation weiterer Gruppen von Patches ermöglicht wird.

Sammlung

Sammlungen sind eine Freiformauswahl *einzelner Rechner-IDs innerhalb einer Ansicht*. Es spielt keine Rolle, zu welchen Gruppen die Rechner-IDs gehören, solange der VSA-Benutzer Zugriff auf diese Gruppen besitzt. Dies ermöglicht dem VSA-Benutzer, logische Sammlungen verwandter Rechner-IDs, wie etwa Laptops, Workstations, Server, MS Exchange Server usw., anzuzeigen und darüber Bericht zu geben. Sammlungen werden durch Aktivieren des Kontrollkästchens **Nur ausgewählte Rechner-IDs zeigen** in **Definitionen anzeigen** *(siehe 27)* erstellt. Speichern Sie eine Ansicht, bevor Sie mit dieser Option Rechner-IDs auswählen. Sobald eine Ansicht gespeichert wurde, wird rechts von dieser Option ein Link **<N> Rechner ausgewählt** angezeigt. Klicken Sie auf diesen Link, um das Fenster **Sammlung definieren** anzuzeigen, in dem Sie mithilfe einer Freiformauswahl einzelner Rechner-IDs eine Ansicht erstellen können.

> **Hinweis:** Die Option **Zusammengeführte Tabelle filtern** *(siehe 30)* bietet eine alternative Möglichkeit, Rechner-IDs für eine Ansichtsdefinition basierend auf standardmäßigen und benutzerdefinierten Attributen auszuwählen.

Schnellansicht

Wenn Sie den Cursor auf ein Check-in-Symbol bewegen, wird sofort das **Agent-Schnellansichtsfenster** geöffnet. Im **Agent-Schnellansichtsfenster** können Sie Agent-Verfahren starten, Protokolle anzeigen oder **Live-Connect** starten. Mithilfe von **Agent-Zeichen** *(siehe 18)* können Sie Text für **besondere Anweisungen** am unteren Rand des **Schnellansichtsfensters** anzeigen.

Schnellstatus

Mithilfe der Funktion **Schnellstatus** können Sie einen *beliebigen* Monitorset-Zähler, -Dienst oder -Prozess für eine *beliebige* Rechner-ID auswählen und sie zum gleichen Einzelanzeigefenster hinzufügen. Mithilfe von **Schnellstatus** können Sie im Handumdrehen die Leistung des gleichen Zählers, Dienstes oder Prozesses auf mehreren Rechnern vergleichen und verschiedene Monitor-Sets in einer einzelnen Ansicht anzeigen. SNMP-Sets stellen eine ähnliche **Schnellstatus**-Ansicht für ausgewählte SNMP-Objekte zur Verfügung. *Eine von Ihnen erstellte Schnellstatus-Ansicht existiert nur für die aktuelle Sitzung.* Sie können das **Schnellstatus**-Fenster aufrufen, indem Sie auf der Seite Monitor > Dashboard > **Monitorset-Status** *(siehe 256)* auf die Verknüpfung **Schnellstatus** oder das Symbol

Schnellstatus klicken.

SNMP-Community

Eine SNMP-Community ist eine Gruppierung von Geräten und Managementstationen, auf denen SNMP ausgeführt wird. SNMP-Informationen werden an alle Mitglieder der gleichen Community in einem Netzwerk gesendet. Die Standard-SNMP-Communities sind:

- Write = privat
- Read = öffentlich

SNMP-Geräte

Bestimmte Netzwerkgeräte wie Drucker, Router, Firewalls, Server und UPS-Geräte bieten keine Unterstützung für die Installation eines **Agent** *(siehe 611)*. Ein VSA-Agent, der auf einem verwalteten Rechner im gleichen Netzwerk wie das Gerät installiert ist, kann jedoch durch Verwendung des **Simple Network Management Protocol (SNMP)** von diesem Gerät lesen bzw. darauf schreiben.

SNMP-Schnellsets

Auf der Seite **SNMP-Info** wird eine Liste der MIB-Objekte angezeigt, die von dem jeweils ausgewählten SNMP-Gerät bereitgestellt werden. Diese MIB-Objekte werden durch Ausführen eines beschränkten SNMP-Durchlaufs auf allen ermittelten SNMP-Geräten ermittelt, wann immer ein **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* stattfindet. Sie können die Liste der ermittelten MIB-Objekte verwenden, um sofort ein gerätespezifisches SNMP-Set mit der Bezeichnung **Schnellset** zu erstellen und auf das Gerät anzuwenden. Schnellsets entsprechen nach der Erstellung den Standardsets. Sie werden in Ihrem privaten Ordner in Monitor > **SNMP-Sets** und in der Dropdown-Liste in Monitor > **SNMP zuweisen** angezeigt. Ein `(QS)`-Präfix erinnert Sie daran, wie das Schnellset erstellt wurde. Wie beliebige andere Standardsets können Schnellsets für ein einzelnes Gerät *individualisiert*, mit Auto-Lernen verwendet, für andere Benutzer freigegeben und über den VSA auf ähnliche Geräte angewendet werden.

1. Ermitteln Sie SNMP-Geräte über Monitor > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor > **SNMP zuweisen** *(siehe 340)* den ermittelten Geräten zu.
3. Klicken Sie auf der Seite **SNMP zuweisen** auf den Hyperlink unterhalb des Namens des Geräts (**SNMP-Info** *(siehe 345)*-Link), um einen Dialog anzuzeigen.
   - Klicken Sie auf **Gefundene MIB-Objekte** und wählen Sie mindestens ein MIB-Objekt aus, das auf dem gerade ausgewählten SNMP-Gerät gefunden wurde.
   - Klicken Sie auf **Schnellset-Elemente** und bearbeiten Sie bei Bedarf die Alarmschwellenwerte für ausgewählte MIB-Objekte.
   - Geben Sie in der Kopfzeile des Dialogfelds den Namen nach dem Präfix **(QS)** ein.
   - Klicken Sie auf die Schaltfläche **Anwenden**, um das Schnellset auf das Gerät anzuwenden.
4. Zeigen Sie vom Schnellset zurückgegebene SNMP-Monitordaten über Monitor > **SNMP-Protokoll** *(siehe 349)* genau so an, wie Sie es bei einem anderen Standard-SNMP-Set tun würden.
5. Die Pflege des neuen Schnellsets kann wahlweise mit Monitor > **SNMP-Sets** *(siehe 629)* erfolgen.

SNMP-Sets

Ein SNMP-Set ist ein Satz von MIB-Objekten, mit denen Sie die Leistung **SNMP-aktivierter Netzwerkgeräte** *(siehe 629)* überwachen können. Das SNMP-Protokoll wird benutzt, weil auf diesen Geräten kein Agent installiert werden kann. Sie können jedem Leistungsobjekt in einem SNMP-Set Alarmschwellenwerte zuweisen. Wenn Sie dem SNMP-Set einem Gerät zuweisen, werden Sie benachrichtigt, wenn der Alarmschwellenwert überschritten wird. Anhand der folgenden Methoden können Sie SNMP-Sets definieren und Rechner-IDs zuweisen.

- **SNMP-Schnellsets** – Erstellt ein gerätespezifisches SNMP-Set basierend auf den beim einem LAN-Watch auf diesem Gerät ermittelten Objekten und weist es zu. **SNMP-Schnellsets** *(siehe 629)* sind die einfachste Methode, SNMP-Monitoring auf einem Gerät zu implementieren.

- **SNMP-Standardsets** – Hierbei handelt es sich für gewöhnlich um generische SNMP-Sets, die auf mehrere Geräte angewendet und auf diesen gepflegt werden. Nachdem ein Schnellset erstellt wurde, kann dieses als ein Standardset gepflegt werden.
- **Individualisierte SNMP-Sets** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann manuell angepasst wurden.
- **SNMP-Auto-Lernen** – Damit bezeichnet man SNMP-Standardsets, die auf ein einzelnes Gerät angewendet und dann automatisch über Auto-Lernen angepasst wurden.
- **SNMP-Typen** – Damit bezeichnet man eine Methode, SNMP-Standardsets, basierend auf dem während eines LAN-Watch festgestellten **SNMP-Typ** *(siehe 630)*, automatisch Geräten zuzuweisen.

In der Regel verwenden Sie das folgende Verfahren, um SNMP-Sets zu konfigurieren und Geräten zuzuweisen.

1. Ermitteln Sie SNMP-Geräte über Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor >**SNMP zuweisen** *(siehe 340)* den ermittelten Geräten zu. Diese können SNMP-Schnellsets, -Standardsets, individualisierte oder Auto-Lernen-Sets einschließen.
3. Zeigen Sie SNMP-Alarme mit Monitor > **SNMP-Protokoll** *(siehe 349)* oder **Dashboard-Liste** *(siehe 251)* an.

Die folgenden zusätzlichen SNMP-Funktionen stehen zur Verfügung und können in beliebiger Reihenfolge verwendet werden.

- Überprüfen Sie wahlweise die Liste aller importierten SNMP-Objekte mit Monitor > **Monitorlisten** *(siehe 264)*.
- Die Pflege von SNMP-Sets kann wahlweise mit Monitor > **SNMP-Sets** *(siehe 276)* erfolgen.
- Mit Monitor > **SNMP-Objekt hinzufügen** *(siehe 281)* können Sie wahlweise ein SNMP-Objekt hinzufügen.
- Mit Monitor > **SNMP-Typ konfigurieren** *(siehe 352)* können Sie wahlweise manuell einen SNMP-Typ einem SNMP-Gerät zuweisen.
- Mit Monitor > **SNMP-Werte einstellen** *(siehe 350)* können Sie wahlweise Werte auf SNMP-Geräte schreiben.

SNMP-Typen

Die meisten SNMP-Geräte werden mithilfe des MIB-Objekts `system.sysServices.0` als ein bestimmter SNMP-Gerätetyp klassifiziert. Beispielsweise identifizieren sich einige Router selbst generisch als Router, indem sie den Wert `77` für das MIB-Objekt `system.sysServices.0` zurückgeben. Sie können den vom MIB-Objekt `system.sysServices.0` zurückgegebenen Wert verwenden, um SNMP-Sets automatisch zu Geräten zuzuweisen, sobald sie von einem LAN-Watch erkannt wurden.

> **Hinweis:** Die gesamte OID für `system.sysServices.0` ist `.1.3.6.1.2.1.1.7.0` oder `.iso.org.dod.internet.mgmt.mib-2.system.sysServices`.

Weisen Sie folgendermaßen **SNMP-Sets** *(siehe 629)* bestimmten **Geräten** *(siehe 629)* *automatisch nach Typ* zu:

1. Fügen Sie SNMP-*Typen* über die Registerkarte **SNMP-Gerät** in Monitor > **Monitorlisten** *(siehe 264)* hinzu bzw. bearbeiten Sie sie.
2. Fügen Sie den vom MIB-Objekt `system.sysServices.0` zurückgegebenen *und mit dem jeweiligen SNMP-Typ verknüpften* Wert hinzu bzw. bearbeiten Sie ihn mithilfe der Registerkarte **SNMP-Dienste** in Monitor > **Monitorlisten**.
3. Verknüpfen Sie einen SNMP-*Typ* über die Dropdown-Liste **Automatische Bereitstellung auf** in Monitor > SNMP-Sets > **SNMP-Set definieren** *(siehe 278)* mit einem SNMP-*Set*.
4. Führen Sie einen **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/7000000/index.asp#1944.htm)* durch. Während des LAN-Watch werden SNMP-Sets automatisch zugewiesen, um von SNMP-Sets überwacht zu werden, wenn das SNMP-Gerät einen Wert für das MIB-Objekt

`system.sysServices.0` zurückgibt, der dem SNMP-Typ entspricht, der mit diesen SNMP-Sets verknüpft ist.

Weisen Sie folgendermaßen **SNMP-Sets** *(siehe 629)* bestimmten **Geräten** *(siehe 629)* *manuell* zu:

- Mit Monitor > **SNMP-Typ konfigurieren** *(siehe 352)* können Sie einen SNMP-Typ einem SNMP-Gerät zuweisen. In diesem Fall beginnt das System automatisch mit dem Monitoring dieses SNMP-Geräts anhand dieses SNMP-Sets.

Software as a Service (SaaS)

Kaseya bietet eine Software-as-a-Service (SaaS)-Bereitstellung von **Virtual System Administrator™** an. Dienstanbieter gehen eine vertragliche Beziehung mit Kaseya für den Zugriff auf einen von Kaseya gehosteten und gewarteten VSA ein und können eine bestimmte Anzahl ihrer Kunden-Agents installieren. Ihnen wird eine eindeutige *Tenant-Partition* eines gemeinsam genutzten Kaseya Server und einer Datenbank zugewiesen. Innerhalb ihrer zugewiesenen Partition können Dienstanbieter nur ihre eigenen Unternehmen, Rechnergruppen, Verfahren, Berichte und Tickets sehen. Die Dienstanbieter in einer Tenant-Partition haben vollen Zugriff auf alle Funktionen des VSA, mit Ausnahme der Systemwartung, die der Verantwortung von Kaseya unterliegt. Weitere Informationen finden Sie im Abschnitt **Lokal** *(siehe 620)*.

Syslog

Syslog ist ein Standard zum Weiterleiten von Protokollnachrichten in einem IP-Netzwerk an einen Syslog-Server. Ein Syslog-Server sammelt die von verschiedenen Geräten im Netzwerk gesendeten Nachrichten und integriert sie in einem zentralisierten Repository von Syslog-Dateien. Syslog ist weit verbreitet bei Unix-, Linux- und Apple-Betriebssystemen sowie Hardwaregeräten wie Cisco-Routern. **Protokollkontrolle** *(siehe 626)* ermöglicht Ihnen die Überwachung von Syslog-Dateien.

Syslog-Dateieinträge haben typischerweise das folgende Format:

```
<time> <hostname> <tag>:<message>
```

Zum Beispiel:

```
Oct 15 19:11:12 Georges-Dev-Computer kernel[0]: vmnet: bridge-en1: interface en is going DOWN
```

Systemablage

Die Systemablage befindet sich standardmäßig in der Taskleiste in der unteren rechten Ecke des Windows-Desktops. Sie enthält die Systemuhr und sonstige Systemsymbole.

System-Agent-Verfahren

Systemagent-Verfahren sind grundlegende Funktionen, die vom VSA angezeigt werden. Sie können planen, dass System-Agent-Verfahren automatisch ausgeführt werden. Sie können jedoch nicht bearbeitet werden und sie akzeptieren auch keine Parameter. Eine Liste der verfügbaren System-Agent-Verfahren wird in einem Popup-Fenster 'Nach Agent-Verfahren suchen' angezeigt. System-Agent-Verfahren können folgendermaßen ausgeführt werden:

- Innerhalb eines übergeordneten Verfahrens mit den Verfahrensbefehlen **execute**Procedure() oder **schedule**Procedure() einer **IF-ELSE-STEP** *(siehe 97)*-Anweisung.
- Über eine beliebige Meldungsseite durch Aktivieren des Kontrollkästchens **Agent-Verfahren ausführen**.
- Über die Registerkarte **Anstehende Verfahren** in **Live Connect** *(siehe 393)* oder auf der Seite **Rechnerübersicht** *(siehe 151)*.

Da ein Systemagent-Verfahren über eine Meldung oder ein übergeordnetes, mit einem bestimmten Rechner-ID-Konto verknüpftes Agent-Verfahren ausgeführt werden kann, lässt sich die Planung eines Systemagent-Verfahrens kopieren. In der Regel erfolgt dies von einer Rechner-ID-Vorlage auf einen Rechner über Agent > **Einstellungen kopieren** *(siehe 62)*.

Systemprüfungen

Der VSA kann auch Rechner überwachen, *auf denen kein Agent installiert ist*. Diese Funktion wird auf

einer einzelnen Seite namens **Systemprüfung** durchgeführt. Rechner ohne einen Agent werden als **externe Systeme** bezeichnet. Einem Rechner mit einem Agent wird die Aufgabe zugewiesen, die Systemprüfung auf dem externen System durchzuführen. Durch eine Systemprüfung wird normalerweise festgestellt, ob ein externes System verfügbar ist oder nicht. Es gibt folgende Arten von Systemprüfungen: Webserver, DNSserver, Portverbindung, Ping und benutzerdefiniert.

Verwalteter Rechner

Ein überwachter Rechner, auf dem ein **Agent** *(siehe 611)* installiert ist und der über ein aktives **Rechner-ID/Gruppen-ID** *(siehe 627)*-Konto auf dem Kaseya Server verfügt. Jeder verwaltete Rechner verbraucht eine **Agent-Lizenz** *(siehe 438)*.

Virtuelle Maschine

Ein virtueller Rechner (Virtual Machine, VM) ist eine Software-Implementierung eines physikalischen Computers (Rechner), die genauso wie ein physikalischer Computer Programme ausführt. Virtuelle Rechner sind in der Lage, einen kompletten Satz von Hardwareressourcen, einschließlich eines Prozessors (oder Prozessoren), Arbeitsspeicher und Speicherressourcen sowie Peripheriegeräten, zu virtualisieren. Das **Sicherungs**modul kann ein Sicherungsabbild in einen VM konvertieren. Siehe Backup > Bild konvertiert in VM.

Virtuelles Netzwerk-Computing (VNC)

Das **virtuelle Netzwerk-Computing (VNC)** wird auch als **Fernsteuerung** oder **Remote-Desktop** bezeichnet. Es ist ein grafisches System zur gemeinsamen Nutzung von Desktops, das das Remote Framebuffer (RFB)-Protokoll zur Fernsteuerung anderer Computer verwendet. Es überträgt die Tastatur- und Mausereignisse von einem Computer zum anderen, wobei die grafischen Bildschirmaktualisierungen über ein Netzwerk zurück in die andere Richtung gesendet werden. Es ist im Lieferumfang des Kaseya Server enthalten und dient hauptsächlich zur Bereitstellung von sofortigem technischem Support. VNC ist plattformunabhängig. Normalerweise kann ein VNC-Viewer auf einem beliebigen Betriebssystem eine Verbindung mit einem VNC-Server auf einem anderen Betriebssystem herstellen. Der **VNC-Server** ist das Programm auf dem Remote-Rechner, der seinen Bildschirm gemeinsam nutzt. Der **VNC-Client (oder Viewer)** ist das Programm auf dem lokalen Rechner, das den Remote-Rechner überwacht und mit ihm interagiert. Der VNC-Clientrechner erfordert Benutzerzugriffsrechte für den VNC-Serverrechner. Da Kaseya-VNC-Sitzungen über den Kaseya Server übermittelt werden, sind alle VNC-Sitzungen durch das Kaseya-256-Bit-Protokoll mit Rolling-Code-Verschlüsselung geschützt.

vPro

Intel® vPro™ Technologie stellt hardwarebasierte Managementintegration unabhängig von der Betriebssystem- und Netzwerkmanagementsoftware zur Verfügung. Der VSA kann vPro-aktivierte Rechner während eines **LAN Watch** *(siehe 620)* erkennen, die Hardwarebestandteile von vPro-Rechnern auflisten, auf hardwarebasierte Sicherheit zugreifen sowie die von vPro bereitgestellten Funktionen für das Energiemanagement und den Remote-Start von ISO-Abbildern verwenden.

Inhaltsverzeichnis

6

A

B

U

V

W

Z